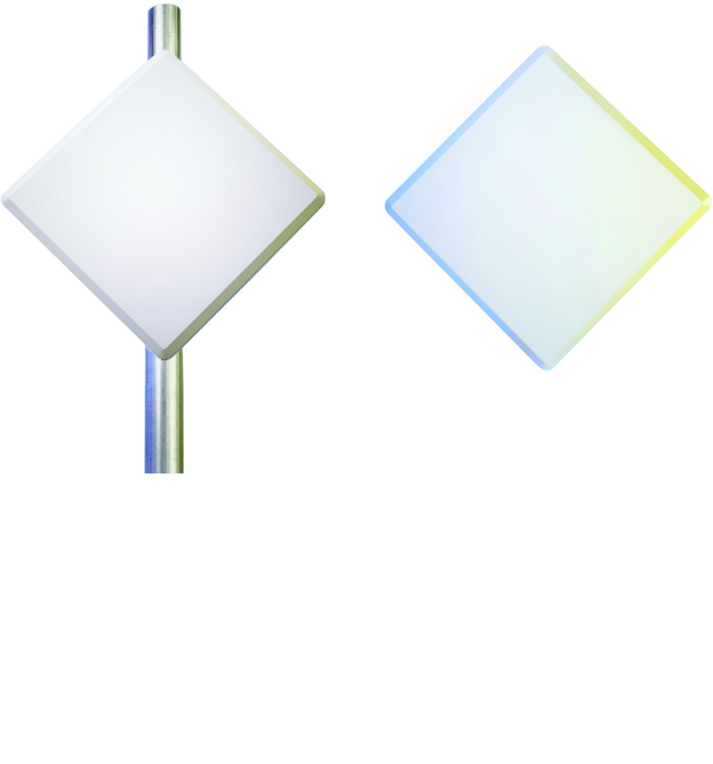
Tsunami MP.11
Model 5054-R and 2454-R
Installation and Management



proxim wireless

IMPORTANT!
Before installing and using this product, see the
Safety and Regulatory Compliance Guide located on the product CD.

Copyright

Trademarks

Tsunami MP.11 2454-R and 5054-R Installation and Management Guide
P/N 73080/1 August 2006

Contents

Introduction

1

The Tsunami MP.11 Model 5054-R (hereinafter referred to as the 5054-R) and the Model 2454-R (hereinafter referred to as the 2454-R) are flexible wireless outdoor routers that let you design solutions for point-to-point links and point-to-multipoint networks.

The 5054-R and 2454-R are both part of the Tsunami MP.11 product family, which is comprised of several additional products, including the 5054 Base Station (BSU), the 5054 Subscriber Unit (SU), and the 5012-SUI for indoor installation. Some of the key features of the product family are:

Some of the key features of the units are:

- The use of a highly optimized protocol for outdoor applications
- Routing and bridging capability
- Asymmetric bandwidth management
- Management through a Web Interface, a Command Line Interface (CLI), or Simple Network Management Protocol (SNMP)
- Software and configuration upgrade through file transfer (TFTP)
- Outdoor placement, close to the antenna, for significantly improved range and ease of installation
- Optional integrated antenna
- VLAN support

About This Book

Before installing and using the unit, Proxim recommends you review the following chapters of this manual:

- **Chapter 1 “Introduction” (this chapter):** Provides an overview of the content of this manual as well as wireless network topologies and combinations that can be built with the unit.
- **Chapter 2 “Installation and Intialization”:** Provides detailed installation instructions and explains how to access the unit for configuration and maintenance.
- **Chapter 3 “System Overview”:** Provides a high-level overview of configuration processes and features.
- **Chapter 4 “Basic Management”:** Explains the most common settings used to manage the unit.
- **Chapter 5 “System Status”:** Depicts the Web Interface’s “Status” options, including System Status and Event Logs.
- **Chapter 6 “Configuration”:** Depicts the Web Interface’s “Configure” options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 7 “Monitoring”:** Depicts the Web Interface’s “Monitor” options in a hierarchical manner, so you can easily find details about each item
- **Chapter 8 “Commands”:** Depicts the Web Interface’s “Commands” options in a hierarchical manner, so you can easily find details about each item
- **Chapter 9 “Procedures”:** Provides a set of procedures, including TFTP Server Setup, Configuration Backup, Restore, and Download, Forced Reload, and Reset to Factory Defaults.
- **Chapter 10 “Troubleshooting”:** Helps you to isolate and solve problems with your radio unit.

The appendixes contain supplementary information you may not need immediately, including Country Code Tables and Technical Support information.

NOTE: *If you are already familiar with this type of product, you can use the Quick Install Guide to install the unit.*

Reference Manual

As a companion to the *Installation and Management* manual, the *Tsunami MP.11 Reference Manual* provides the following supplemental information:

- **Command Line Interface:** Documents the text-based configuration utility’s keyboard commands and parameters.
- **Event Log Error Messages:** Documents the error messages that you may see in your Event Log.
- **Alarm Traps:** Documents the alarm traps that can be set.
- **Microsoft Windows IAS Radius Server Configuration:** Provides information to assist you in setting up the IAS Radius Server.
- **Addition of Units to a Routed Network:** Describes how to add more units to your routed network.
- **Glossary:** Describes terms used in the Tsunami MP.11 documentation and in the wireless industry.

Wireless Network Topologies

The unit can be used in various network topologies and combinations. The required equipment depends upon the wireless network topology you want to build. Make sure all required equipment is available before installing the unit.

The 5054-R and 2454-R are designed for outdoor placement. One model of the SU is equipped with an integrated antenna. For all other models, you can connect the unit to an outdoor antenna. See the *Tsunami MP.11 Antenna Installation Guide* for details.

WARNING: To connect the unit to an outdoor antenna, consult the appropriate manufacturers' documentation for additional regulatory information, safety instructions, and installation requirements.

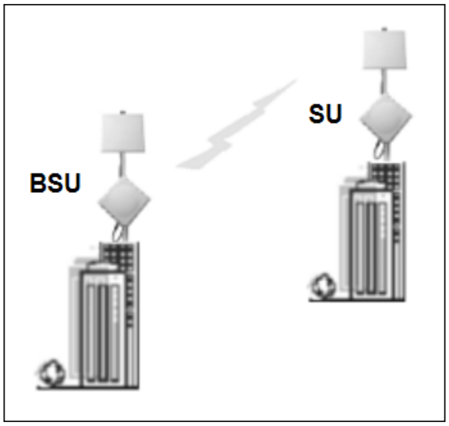
You can set up the following types of topologies:

- Point-to-Point Link
- Point-to-Multipoint Network

Each unit is set up as either a Base Station Unit (BSU) or a Subscriber Unit (SU). A link between two locations always consists of a BSU and an SU. A BSU can, depending upon its configuration, connect to one or more SUs. An SU, however, can connect only to one BSU.

Point-to-Point Link

With a BSU and an SU, it is easy to set up a wireless point-to-point link as depicted in the following figure.

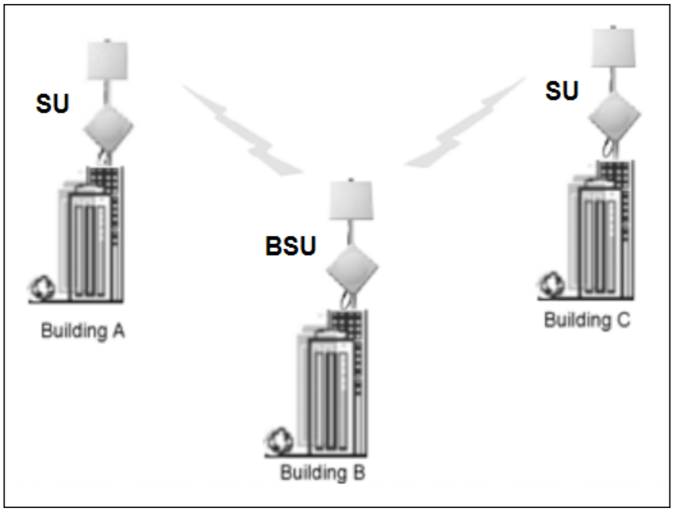


A point-to-point link lets you set up a connection between two locations as an alternative to:

- Leased lines in building-to-building connections
- Wired Ethernet backbones between wireless access points in difficult-to-wire environments

Point-to-Multipoint Network

If you want to connect more than two buildings, you can set up a single point-to-multipoint network with a single BSU and multiple SUs, as depicted in the following figure.



Up to 250 SUs can be connected to a BSU. If a BSU already has 250 SU, a new SU cannot be connected to the BSU. In this figure, the system is designed as follows:

- The central building **B** is equipped with a BSU, connected to either an omni-directional, or a wide angle antenna.
- The two other buildings **A** and **C** are both equipped with an SU connected to a directional antenna.

Power-over-Ethernet

The unit is equipped with an Active Ethernet module. Using Power-over-Ethernet (PoE), you can provide electricity and wired connectivity to the unit over a single Category 5 cable. Although the power injector that is supplied with the unit is 802.3af-compatible, standard 802.3af-compliant power modules will not properly power the units. Always use the supplied power injector.

- The Active Ethernet integrated module provides –48 VDC over a standard Cat5 Ethernet cable.
- Maximum power supplied to the unit is 20 Watts (when the unit is heating or cooling); the units typically draw less than 7.5 Watts.
- The unit only accepts power on the “extra pairs”, not on the data pairs according the configuration for “midspan” power injection, see the IEEE 802.3af standard.

Heating or cooling discussion: Between 0 and 55° Celsius internal temperature, the unit does not need to regulate its temperature, so the power draw is generally lower in this temperature range. When the internal temperature gets close to the limits, the unit starts to heat/cool itself and the power draw increases. Powering while cold triggers a special self-heat mode where the unit is inoperable until the temperature is above 0° deg Celsius. This is signaled by a solid red LED on the Ethernet connector. Once the internal temperature is above 0 degrees Celsius, the unit boots normally.

Management and Monitoring Capabilities

There are several management and monitoring interfaces available to the network administrator to configure and manage the unit:

- Web Interface
- Command Line Interface
- SNMP Management

Web Interface

The Web interface (HTTP) provides easy access to configuration settings and network statistics from any computer on the network. You can access the Web interface over your network, over the Internet, or with a crossover Ethernet cable connected directly to your computer’s Ethernet port. See Logging in to the Web Interface.

Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage the unit. You enter command statements, composed of CLI commands and their associated parameters. You can issue commands from the keyboard for real-time control or from scripts that automate configuration. See the *Tsunami MP.11 Reference Manual* for more information about the Command Line Interface.

SNMP Management

In addition to the Web interface and the CLI, you also can manage and configure your unit using the Simple Network Management Protocol (SNMP). Note that this requires an SNMP manager program (sometimes called MIB browser) or a Network Manager program using SNMP, such as HP OpenView or Castelrock’s SNMPc. The units support several Management Information Base (MIB) files that describe the parameters that can be viewed and configured using SNMP:

- mib802.mib
- orinoco.mib
- rfc1213.mib
- rfc1493.mib
- rfc1643.mib

Proxim provides these MIB files on the CD included with your unit. You must compile one or more of these MIB files into your SNMP program's database before you can manage your unit using SNMP. See the documentation that came with your SNMP manager for instructions about how to compile MIBs.

NOTE: *When you update the software in the unit, you must also update the MIBs to the same release. Because the parameters in the MIB may have changed, you will not otherwise have full control over the features in the new release.*

The enterprise MIB (orinoco.mib) defines the read and read/write objects you can view or configure using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. See the enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word, Notepad, and WordPad. See SNMP Parameters.

IMPORTANT!

Using a serial connection, you can access the unit through a terminal emulation program such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP.11 Reference Manual*.)

For all other modes of connection, you will need the IP address of the unit in order to use the Web Interface, SNMP, or the CLI. See Setting the IP Address with ScanTool for more information.

Installation and Initialization 2

This chapter describes the steps required to install and mount the unit, and to align the antenna. An antenna cable is required only when you use the external antenna option. Note that the unit must have either the integrated antenna or must be connected to an external antenna for its operation. The installation procedure does not include the mounting and connection of antennas. See the *Tsunami MP.11 Antenna Installation Guide* for this information.

If you are already familiar with this type of product, you can use the *Quick Install Guide* for streamlined installation procedures.

See the following sections:

Hardware Overview

The 5054-R and 2454-R units contain a state-of-the-art wireless radio, an optional high-gain performance flat-panel antenna, and Power-over-Ethernet (the sole means of power for the unit). For further protection, the unit has internal, built-in surge protection.

Power and Ethernet Connection

Recommended Cable	
Function	Power (DC) and Ethernet connection
Type	Cat5, UV-shielded and outdoor-rated
Impedance	100 ohms
Recommended cables	4 UTP, 24 AWG, UL rated
Maximum Distance	330 feet / 100 meters
Connector type, unit end	RJ45 female, weatherized using weatherproof connector
Connector type, power & Ethernet adapter end	RJ45

Serial Connection

The serial connection is made with an RJ11 to DB9 connector (also referred to as a “dongle”). Connect the RJ11 end to the unit and connect the serial (DB9) end to your PC to assist you in aligning the antenna and to issue CLI commands. See the following figure:

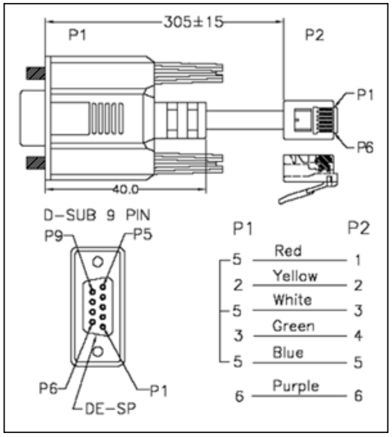


Figure 2-1 Serial Dongle Diagram

The connections are as follows:

D-Shell	RJ11
1	NC
2	2
3	4
4	NC
5	1 + 3 + 5
6	6
7	NC
8	NC
9	NC

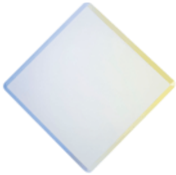
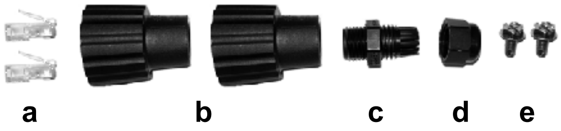
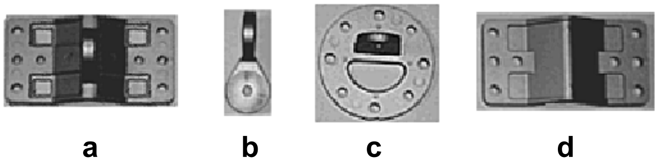
External Antenna Connection

One model of the SU has an integrated antenna; all other models have an external antenna connector (N-type) and no integrated antenna. For more information about external antennas, see the *Antenna Installation Guide*.

Product Package

Each shipment includes the items in the following table. Verify that you have received all parts of the shipment.

NOTE: *Unless noted in this table, cables are not supplied with the unit.*

SU with Integrated Antenna or BSU / SU with external antenna connector	
RJ11 to DB9 Serial Connector (supplied with BSU only)	
Installation CD	
Power Injector and Cord	
Cable Termination Kit	Kit includes the following:  a. RJ45 connectors (2) b. Sealing caps (2) c. Sealing nut d. Lock nut e. Grounding screws
Mounting Kit	Kit includes the following:  a. Mounting clamp for wall/pole b. Extension arm c. Mounting plate to enclosure d. Mounting clamp for pole mounting

<table>
<tr><td>Mounting Hardware</td><td>The following mounting hardware, included with the mounting kit:
<table>
<tr><th><u>Quantity</u></th><th><u>Description</u></th><th></th></tr>
<tr><td>6 ea.</td><td>Plain washer #5/16</td><td> </td></tr>
<tr><td>2 ea.</td><td>Hex Cap Screw NC 5/16-18 x 35</td><td> </td></tr>
<tr><td>2 ea.</td><td>Nut NC 5/16-18</td><td> </td></tr>
<tr><td>4 ea.</td><td>Helical Spring Lock Washer #1/4</td><td> </td></tr>
<tr><td>4 ea.</td><td>Helical Spring Lock Washer #1/16</td><td> </td></tr>
<tr><td>2 ea.</td><td>Hex Cap Screw NC 5/16-18 x 80</td><td> </td></tr>
<tr><td>4 ea.</td><td>68764, Screw, Machine, Pan,
Philips, 1/4"-20, 5/8"L</td><td> </td></tr>
</table>
</td></tr>
</table>

Installation Procedure

IMPORTANT:
Before installing and using this product, see *Safety and Regulatory Compliance Information* on the product CD.

WARNING:
To ensure proper grounding, use the hole at the bottom point on the back of each unit and the provided grounding screws to attach a ground wire of at least 10 AWG stranded to each unit. Use proper wire grounding techniques in accordance with local electric codes.

NOTES:

- *The **Configure System** window provides a selectable **Country** field that automatically provides the allowed bandwidth and frequencies for the selected country as well as, where applicable, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC).*
- *Non-US installers should not add an antenna system until the **Country** is selected, the unit is rebooted, and the proper power level is configured. The output power level of the final channel selected by DFS scan can be found in the Event Log.*
- *Be sure to read the **Release Notes** file on the product CD as it contains software version and driver information that may not have been available when this document was produced.*
- *Equipment is to be used with, and powered by, the power injector provided or by a power injector that meets these requirements:*
  - *UL-Listed/ITE (NWGQ)*
  - *Limited Power Source Output per UL/IEC 60950*
  - *CE-marked*
  - *Approved for Power-over-Ethernet*
  - *Rated output, 48 Vdc/0.42 A*
  - *Pinout follows 802.3af standard for mid-span devices*

Step 1: Choose a Location

To make optimal use of the unit, you must find a suitable location for the hardware. The range of the unit largely depends upon the position of the antenna. Proxim recommends you do a site survey, observing the following requirements, before mounting the hardware.

- The location must allow easy disconnection of the unit from the power outlet if necessary.
- The unit must not be covered and the air must be able to flow freely around the unit.
- The unit must be kept away from vibration, excessive heat, and humidity, and kept free from dust buildup.
- The installation must conform to local regulations at all times.

The units are designed to directly mount to a pole or wall. Using the supplied brackets and hardware, you can mount them to a 1.25 inch to 4.5-inch pole (outside diameter). Using just one of the mounting brackets, you can mount the units to a wall or other flat surface.

CAUTION: *Proxim recommends the use of a lightning arrestor at the building ingress point. You can purchase the Proxim Lightning Protector MP.11/QB.11 (70251); see the documentation that comes with the unit for more information and installation instructions.*

Step 2: Pre-Assemble the Hardware

1. Unpack the unit and accessories from the shipping box.
2. Note the Ethernet and MAC addresses of the SU, as well as the serial number; these addresses may be used when configuring the BSU.

   NOTE: *The serial number is required to obtain support from Proxim. Keep this information in a safe place.*

3. You will be attaching an outdoor-rated 24 AWG CAT5 cable (diameter .114 to .250 inches/2.9 to 6.4 mm) (not provided) to the Power-over-Ethernet port on the back of the unit later in the installation procedure. First, you must construct the cable and assemble the waterproofing cable covers as described in the following steps:

   i. Slide the sealing nut (A) over the bare end of the CAT5 cable.

   ii. Slide the lock nut (B) over the bare end of the CAT5 cable.

   iii. Slide the RJ45 sealing cap (C) over the bare end of the CAT5 cable.

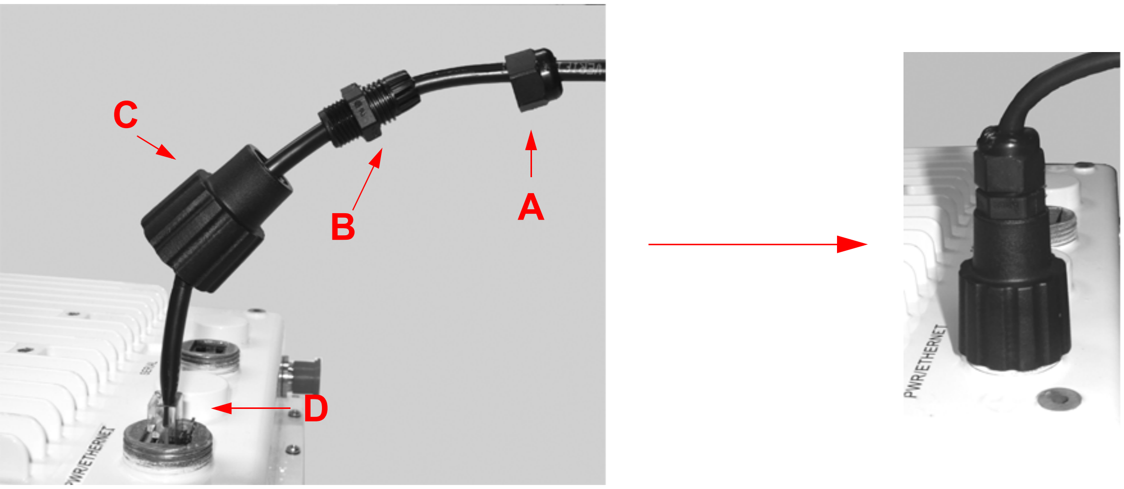
   iv. Terminate the RJ45 connector to the CAT5 cable. Insert into the mating RJ45 connector (D).

   v. Slide the RJ45 sealing cap (C) over the RJ45 connector and thread onto enclosure. Hand tighten.

   vi. Thread the lock nut (B) onto sealing cap (C), and hand tighten.

   vii. Thread the sealing nut (A) onto the lock nut (B), and hand tighten.

   CAUTION: *Hand-tighten only. Torque values for final installation are provided in* Step 8: Complete Installation.

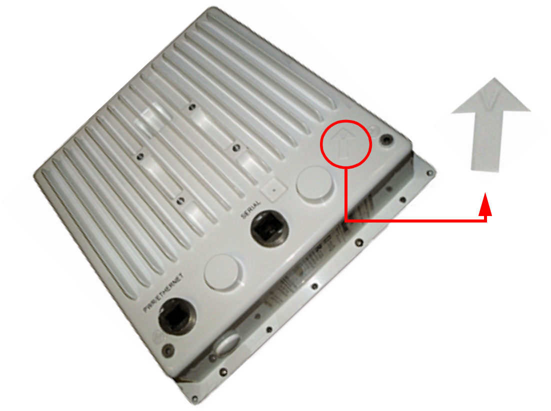


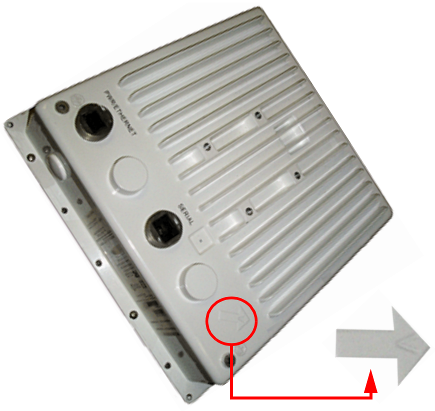
CAUTION: *The sealing nut (A) must not be tightened until the sealing cap (C) over the RJ45 connector has been tightened to the unit during final installation; otherwise, the Ethernet cable may twist and damage.*

NOTES:

- *The cable must feed through all parts of the weatherproof cap before the RJ45 is crimped on the outdoor Ethernet a cable.*
- *The cable between the power injector and the unit must be a straight-through Ethernet cable (without crossover).*
- *Due to variance in CAT5 cable diameter, termination techniques of the installer, and the application of proper tightness of the connectors, it is strongly recommended that the CAT5 cable connector and the serial connector cap are further secured by external weatherproofing (in addition to the antenna N connector, where applicable). Butyl weatherproofing tape is the preferred material for securing any external connector.*

4. Locate the arrow on the back of the unit and determine your desired mounting orientation. For *vertical polarization* using the integrated antenna, the arrow should be pointing up (perpendicular to the ground). For *horizontal polarization* using the integral antenna, the arrow should be horizontal (parallel to the ground).

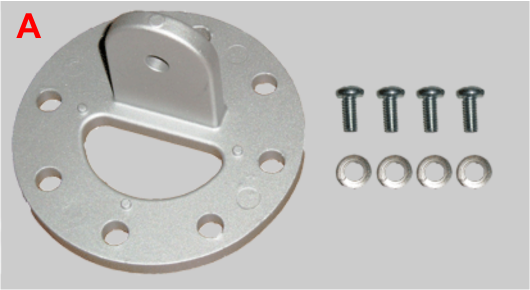


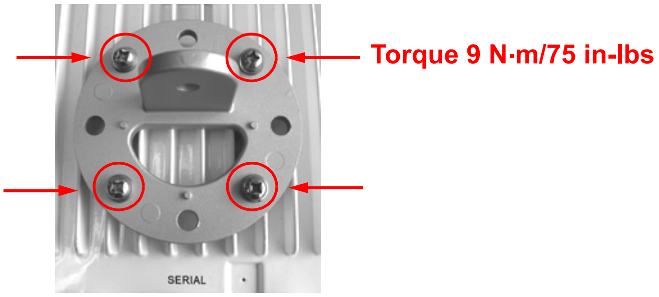


Vertical Polarization

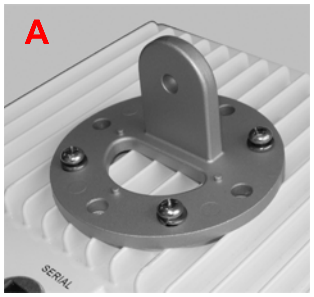
Horizontal Polarization

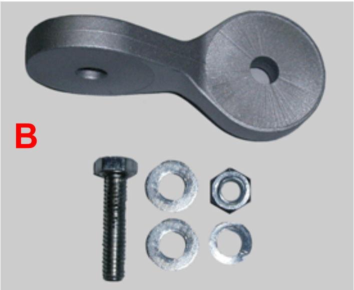
5. Attach the mounting plate (A) using the provided screws and washers (Torque 9 N·m/75 in-lbs), such that the unit's antenna will be vertically or horizontally polarized when mounted.

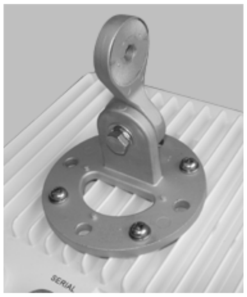




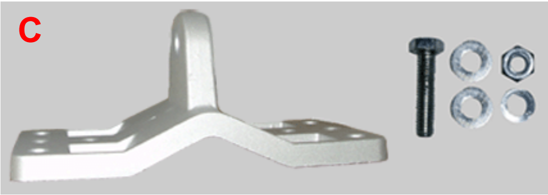
6. Attach the extension arm (B) to mounting piece (A) with the screw, nut, and washers provided, as shown below. The extension arm gives the unit more possible tilt, letting you adjust for azimuth or elevation over a larger angle.

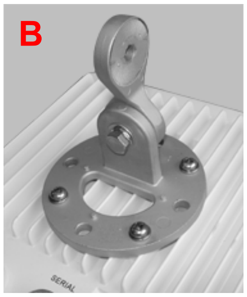


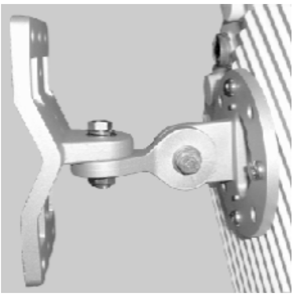




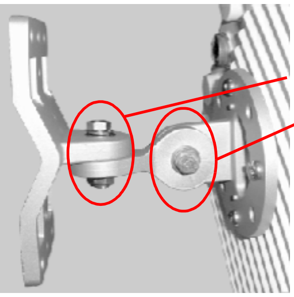
7. Attach the mounting bracket (C) to extension arm (B) with the screw, nut, and washers provided.





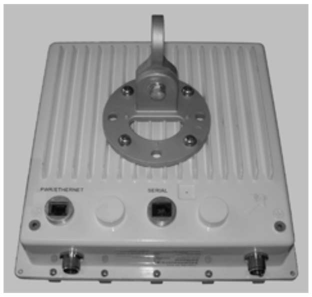


8. Tighten assembly (Torque 15 N·m/130 in-lbs).



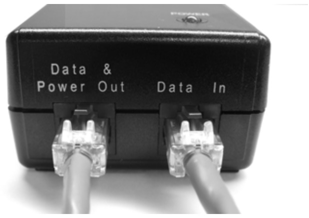
Torque 15 N·m/130 in-lbs

The following figure shows the full assembly attached to the unit:



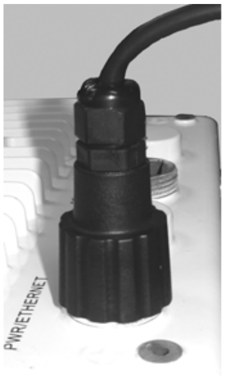
Step 3: Connect the Cables

1. If you have not already done so, connect the normal RJ45 connector on an outdoor-rated CAT5 cable to the “Data and Power Out” port on the power injector.



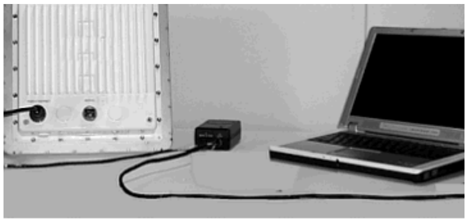
2. Attach the other end of the CAT5 cable with RJ45 connector to the Power and Ethernet port on the back of the unit (see the following figure). Note that the first attachment of this cable is meant to verify operation and configure the unit; the final attachment (with proper torque) and weatherproofing are to be done after the unit has been installed in the location at which it will operate (Step 8: Complete Installation)

   CAUTION: Do not over-tighten the connector nuts; do not use a wrench to tighten the connectors!



3. To connect the unit through a hub or a switch to a PC, use a ***straight-through Ethernet cable*** between the network interface card in the PC and the hub, and between the hub and the RJ45 “Data In” port on the power injector.

   If you are connecting the PC directly to the unit, use a ***crossover Ethernet cable*** between the network interface card in the PC and the RJ45 “Data In” port on the power injector.



Step 4: Power on the Unit

Once you have connected the power injector to the Ethernet cabling and plugged the power injector cord into an AC outlet, the unit is powered on. There is no ON/OFF switch on the unit. To remove power, unplug the AC cord from the AC outlet or disconnect the RJ45 connector from the “Data and Power Out” port on the power injector.

CAUTION: *Proxim recommends the use of a lightning arrestor at the building ingress point. You can purchase the Proxim Lightning Protector MP.11/QB.11 (70251); see the documentation that comes with the unit for more information and installation instructions.*

Step 5: View LEDs

When the unit is powered on, it performs startup diagnostics. When startup is complete, the LEDs show the unit’s operational state. The LEDs are present at the unit’s Ethernet connector; unscrew the watertight cap if necessary to view the LEDs.

NOTE: *Make sure the domed sealing nut is loose before unscrewing the cap or the Ethernet cable may be twisted and become damaged.*

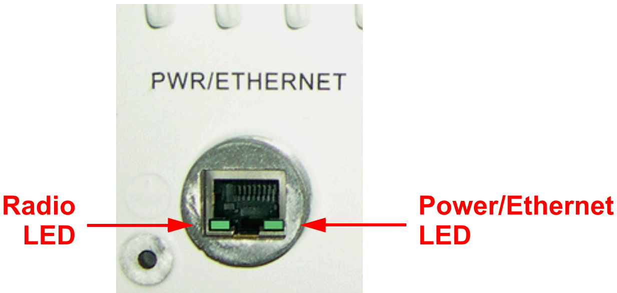


Figure 2-2 LED Indicators on Ethernet Connector

During bootup, all LEDs are blinking. Blinking can continue for up to four minutes (when DFS is enabled, for example); however, if the LEDs are still blinking for over four minutes, you should check your installation and proper operation of the Ethernet and wireless links to other units. If they are correct, contact Technical Support; there could be a problem with your hardware.

NOTE: *When powering the unit in below freezing temperatures, the unit must self-heat before booting. This is indicated by a solid red LED. This state can take up to 30 minutes, depending upon the ambient temperature.*

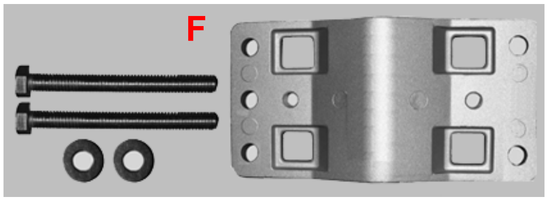
LEDs exhibit the following behavior:

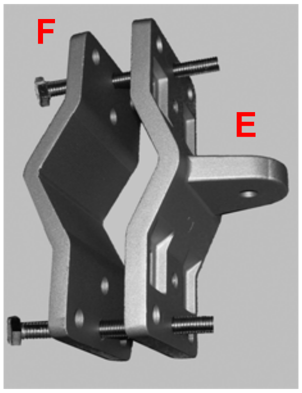
LED State	Radio LED	Power/Ethernet LED
Red	Power is on; unit is self-heating.	—
Flashing Green	Wireless link is being established.	Power is on, Ethernet link is down.
Solid Green	Wireless link has been established.	Power is on, Ethernet link is up.

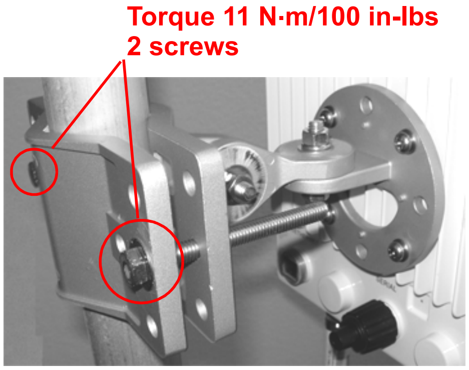
Step 6: Mount the Unit

CAUTION: *To ensure that water does not gather around the antenna connectors, mount the unit with the antenna connectors facing downward*

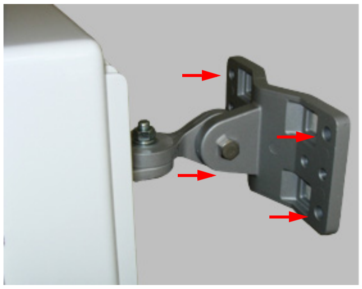
1. To pole-mount, insert screws through bracket F and fasten around pole to bracket E and secure (Torque 11 N·m/100 in-lbs).







2. To wall-mount the unit, mount bracket (E) to wall using 4 screws (not provided), as shown:



Step 7: Align the Antenna

Antenna alignment is the process of physically aligning the antenna of the radio receiver and transmitter to have the best possible link established between them. The antenna alignment process is usually performed during installation and after major repairs.

The unit has an audible antenna alignment tool that can be activated by plugging in the supplied serial dongle (supplied with the BSU) or by issuing the CLI command for antenna alignment. The CLI command causes both audible and numerical feedback as the CLI shows the running Signal-to-Noise Ratio (SNR) values twice a second.

The output from the beeper for antenna alignment consists of short beeps with a variable interval. The interval changes with the SNR level to assist in correctly aligning the antenna. An increase in signal level is indicated by a shorter interval between beeps; a reduction in signal level results in beeps longer apart.

To allow for precise antenna alignment, small changes in SNR result in large changes in the beep period. The alignment process averages the SNR, which is represented by an average length beep. When a higher SNR is received, the beep period is made shorter, dependent upon the difference to the average. A lower SNR results in a longer period between beeps.

The first five steps around the average are represented by a large change and all following steps are a small change. This acts as if a magnifying glass is centered around the average SNR and the values next to the average are significantly different.

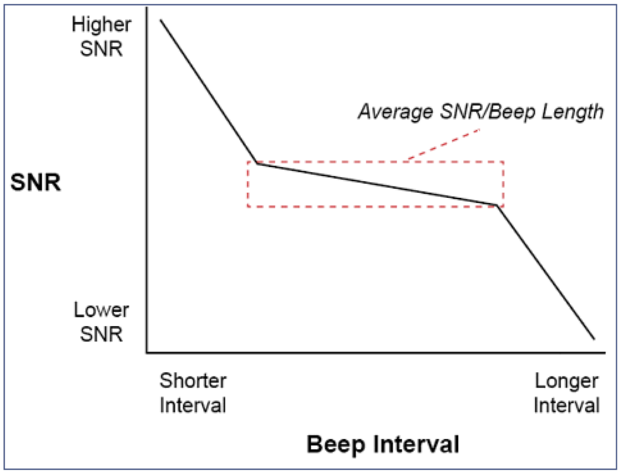


Figure 2-3 SNR and Beep Interval

When the antenna is aimed, the beep intuitively represents whether the SNR is rising or falling: the higher the SNR rises, the shorter the period the beep is heard and the higher the frequency of the beep.

After the position of the antenna has been changed, SNR averaging settles at the new value and the beeping returns to the average length so the antenna can again be aimed for rising SNR.

Aiming is complete if moving in any direction results in a falling SNR value (which can be heard as longer periods between beeps).

NOTES:

- *Antenna alignment for the Base Station is useful only for a point-to-point link.*
- *The range of the average SNR has been limited to values from 5 to 43; therefore, anything over 43 always results in a short period between beeps and values below 5 always have a long period.*

- *The Antenna Alignment Display (AAD) CLI command is disabled automatically 30 minutes after it is enabled to remove the load of extra messages on the wireless interface. The default telnet timeout is 900 seconds (15 minutes). If AAD must run for the entire 30 minutes, change the default telnet timeout value to a value greater than 30 minutes (greater than 1800 seconds). This restriction is for telnet connections only and not for the serial interface. The serial interface never times out; however, the AAD command does still time out.*

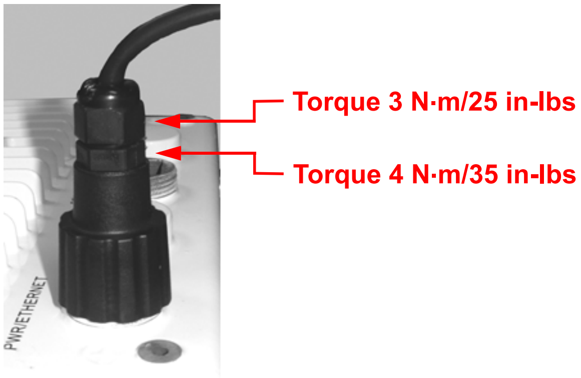
Antenna Alignment Commands

- **`set aad enable local`**: Enables display of the local SNR. Local SNR is the SNR measured by the receiver at the near end.
- **`set aad enable remote`**: Enables display of the remote SNR. Remote SNR is the SNR as measured by the receiver at the far end.
- **`set aad enable average`**: Enables display of the average SNR. The average SNR is the average of the local and remote SNR.
- **`set aad disable`**: Disables Antenna Alignment Display (Ctrl-C also disables AAD).

Step 8: Complete Installation

1. Tighten the sealing nut (Torque 3 N·m/25 in-lbs) and lock nut (Torque 4 N·m/35 in-lbs).

   CAUTION: *Do not over-tighten. Over-tightening can cause the CAT5 cable to crush and can subsequently damage the power injector or the unit.*



2. Tighten the RJ45 sealing cap.

CAUTION: *Be sure you have re-installed the waterproof caps on the serial and Ethernet port connections. It is also good installation practice to use Butyl weatherproofing tape to seal the caps, as this adds an extra layer of protection.*

Step 9: Install Documentation and Software

To install the documentation and software on a computer or network:

1. Place the CD in a CD-ROM drive. The installer normally starts automatically. (If the installation program does not start automatically, click **setup.exe** on the installation CD.)
2. Click the Install Software and Documentation button and follow the instructions displayed on the installer windows. The following documentation and software products are installed:
   - Available from **Start > All Programs > Tsunami > MP.11 5054R-2454R**:
     - Documentation (in **Docs** subdirectory):
       - Installation and Management Guide
       - Quick Installation Guide
       - Reference Manual
       - Safety and Regulatory Guide
       - Recommended Antenna Guide
       - Antenna Installation Guide
       - Release Notes
     - MP.11 5054-R/2454-R Online Help
     - Scan Tool (in **Scan Tool** subdirectory)
     - TFTP Server (in **TFTP Server** subdirectory)

     NOTE: *All of these items are slso Available from* ***C:\Program Files\Tsunami\MP.11 5054R-2454R****.*
   - Available from **C:\Program Files\Tsunami\MP.11 5054R-2454R**:
     - Scan Tool program
     - Documentation (in **Docs** folder): See list above
     - Help files (in **Help** folder; click on index.htm to access)
     - **Extras** folder containing TFTP Server and Scan Tool program
     - MIBs (in **MIBs** folder)
     - Firmware (in **Firmware** folder)

Initialization

Connecting to the unit requires either:

- A direct physical connection with an Ethernet cross-over cable or with a serial RS232C cable
- A network connection

Connecting with a serial connection, allows you to configure and manage the unit with the CLI. Connecting with the other connections allows you to use of the Web Interface and SNMP in addition to the CLI.

Using a serial connection, you can access the unit through a terminal emulation program such as HyperTerminal. (See “HyperTerminal Connection Properties” in the *Tsunami MP.11 Reference Manual*.)

For all other modes of connection, you will need the IP address of the unit in order to use the Web Interface, SNMP, or the CLI. Because each network is different, an IP address suitable for your network must be assigned to the unit. You must know this IP address to configure and manage the unit through its Web Interface, SNMP, or the CLI. The unit can use either a **static** or **dynamic** IP address. The unit either obtains its IP address automatically through DHCP (dynamic IP address) or it must be set manually (static IP address).

ScanTool

With ScanTool (a software utility that is included on the product installation CD), you can find out the current IP address of the unit and, if necessary, change it so that is appropriate for your network. The units are shipped with the static IP address 10.0.0.1 configured.

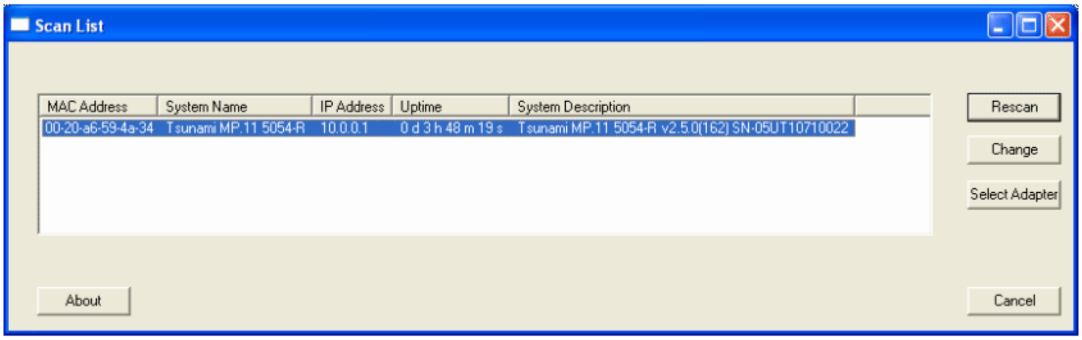
ScanTool lets you find the IP address of a Tsunami MP.11 5054-R or 2454-R by referencing the MAC address in a Scan List, or to assign an IP address if the correct one has not been assigned. The tool automatically detects the units installed on your network segment, regardless of IP address, and lets you configure each unit’s IP settings. In addition, you can use ScanTool to download new software to a unit that does not have a valid software image installed.

Setting the IP Address with ScanTool

To discover and set/change the IP address of the unit:

1. Run ScanTool on a computer connected to the same LAN subnet as the unit, or a computer directly connected to the unit with a cross-over Ethernet cable. Double-click the **ScanTool** icon on the Windows desktop to launch the program. If the icon is not on your desktop, click **Start** > **All Programs** > **Tsunami** > **MP.11 5054R-2454R** > **Scan Tool**.

   ScanTool scans the subnet for 5054-R and 2454-R units and displays a list of the units it finds in the Scan List window (shown below). If necessary, click **Rescan** to re-scan the subnet and update the display.

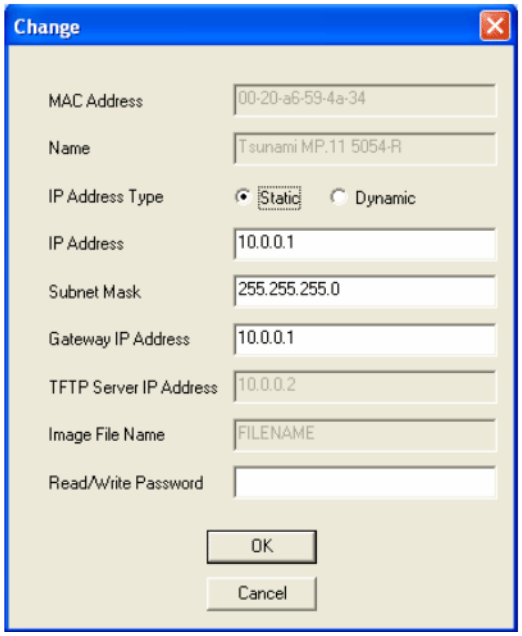


MAC Address	System Name	IP Address	Uptime	System Description
00-20-a6-59-4a-34	Tsunami MP.11 5054-R	10.0.0.1	0 d 3 h 48 m 19 s	Tsunami MP.11 5054-R v2.5.0(162) SN-05UT10710022

Figure 2-4 Scan List

You can assign a new IP address to one unit, even if more than one unit has the same (default) IP address 10.0.0.1, but the new IP address must be unique to allow use of the management interfaces.

2. Select the unit for which you want to set the IP address and click **Change**. The **Change** dialog window is displayed, as shown below.



MAC Address	00-20-a6-59-4a-34
Name	Tsunami MP.11 5054-R
IP Address Type	● Static ○ Dynamic
IP Address	10.0.0.1
Subnet Mask	255.255.255.0
Gateway IP Address	10.0.0.1
TFTP Server IP Address	10.0.0.2
Image File Name	FILENAME
Read/Write Password	

Figure 2-5 Change Window

3. To set the IP address ***manually***, ensure that **Static** is selected as the **IP Address Type** and fill in the **IP Address** and **Subnet Mask** suitable for the LAN subnet to which the unit is connected.

   To set the IP address ***dynamically***, ensure that **Dynamic** is selected as the **IP Address Type**. The unit will request its IP address from a DHCP server on your network.

4. Enter the **Read/Write Password** (the default value is **public**) and click **OK** to confirm your changes. The respective unit reboots to make the changes effective.

   NOTE: *The number of asterisks displayed after you enter the password does not necessarily equal the number of characters in the actual password string. This is done for added security.*

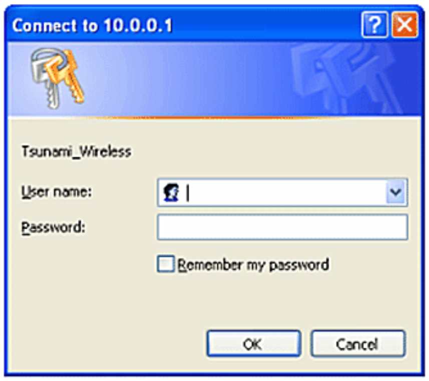
Logging in to the Web Interface

The Web Interface provides a graphical user interface through which you can easily configure and manage the unit. This section describes only how to access the Web Interface.

To use the Web Interface, you need only the IP address of the unit. (See Setting the IP Address with ScanTool for details).

NOTE: *If the connection is slow or you are not able to connect, use the Internet Explorer Tools option to ensure you are not using a proxy server for the connection with your Web browser.*

To access the unit with a Web browser, start your Web browser and enter the IP address of the unit. The Web address must appear as **http://<ip address>** (for example, **http://10.0.0.1**). A window such as the following is displayed.



Connect to 10.0.0.1

Tsunami_Wireless

User name:

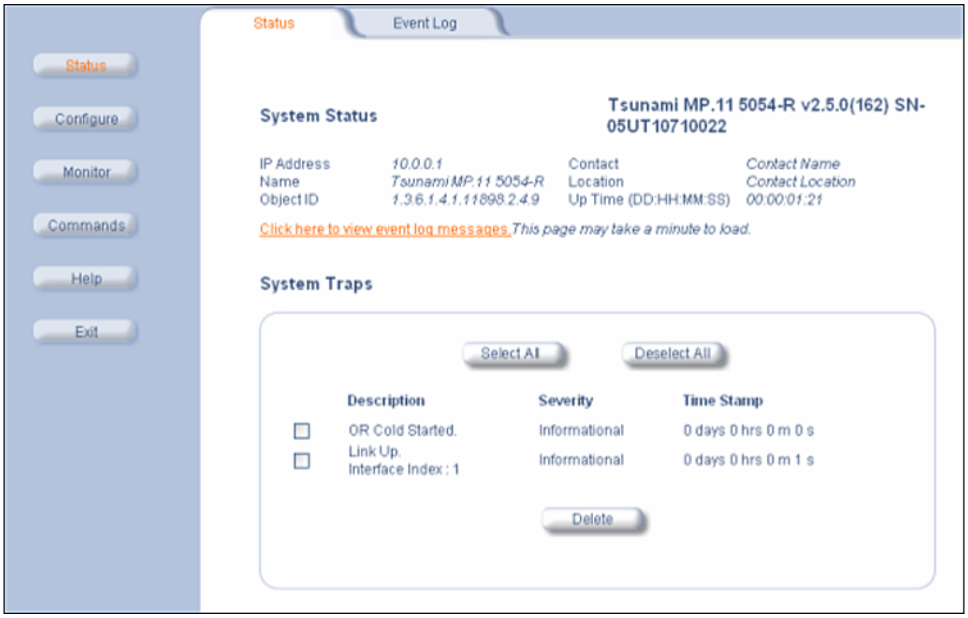
Password:

□ Remember my password

Figure 2-6 Login Window

Do not fill in the **User Name**, enter only the password and click **OK**. The default password is **public**.

The **System Status** window is displayed. To find out more about the information presented in this window, see System Status.



System Status

Tsunami MP.11 5054-R v2.5.0(162) SN-05UT10710022

IP Address	*10.0.0.1*	Contact	*Contact Name*
Name	*Tsunami MP.11 5054-R*	Location	*Contact Location*
Object ID	*1.3.6.1.4.1.11898.2.4.9*	Up Time (DD:HH:MM:SS)	*00:00:01:21*

Click here to view event log messages. *This page may take a minute to load.*

System Traps

	Description	Severity	Time Stamp
□	OR Cold Started.	Informational	0 days 0 hrs 0 m 0 s
□	Link Up. Interface Index : 1	Informational	0 days 0 hrs 0 m 1 s

Figure 2-7 System Status

You now have access to the unit’s Web Interface. The remainder of this manual describes configuring and monitoring the unit using this interface.

3 System Overview

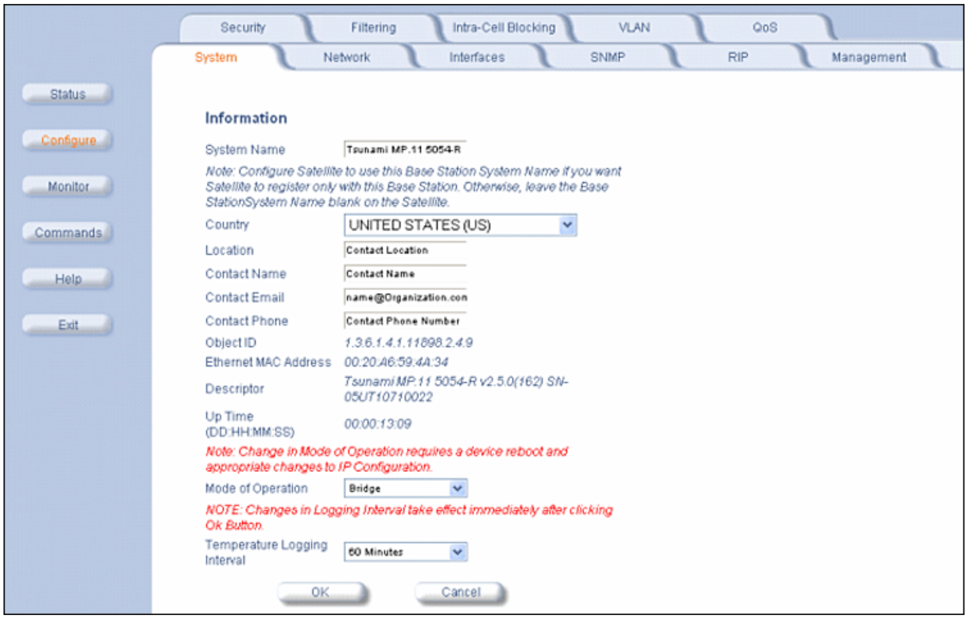
This chapter provides an overview of the system. See the following sections:

- Changing Basic Configuration Information
- SU Registration
- Dynamic Data Rate Selection (DDRS)
- Quality of Service (QoS)

Changing Basic Configuration Information

To view or change basic system information, click the **Configure** button on the left side of the Web interface window, then click the **System** tab. See System Parameters for detailed information about the fields and selections in this window.

NOTE: *System Name by default contains the actual model number. The following screenshot is for information only.*



Information

System Name: Tsunami MP.11 5054-R

Note: Configure Satellite to use this Base Station System Name if you want Satellite to register only with this Base Station. Otherwise, leave the Base StationSystem Name blank on the Satellite.

Country: UNITED STATES (US)

Location: Contact Location

Contact Name: Contact Name

Contact Email: name@Organization.con

Contact Phone: Contact Phone Number

Object ID: 1.3.6.1.4.1.11898.2.4.9

Ethernet MAC Address: 00:20:A6:59:4A:34

Descriptor: Tsunami MP.11 5054-R v2.5.0(162) SN-05UT10710022

Up Time (DD:HH:MM:SS): 00:00:13:09

Note: Change in Mode of Operation requires a device reboot and appropriate changes to IP Configuration.

Mode of Operation: Bridge

NOTE: Changes in Logging Interval take effect immediately after clicking Ok Button.

Temperature Logging Interval: 60 Minutes

Country and Related Settings

The unit's **Configure System** window provides a selectable **Country** field that automatically provides the allowed bandwidth and frequencies for the selected country.

Units sold in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other **Country** can be configured. Units sold outside of the United States support the selection of a **Country** by the professional installer.

NOTE: *Non-US installers should not add an antenna system until the **Country** is selected, the unit is rebooted, and the proper power level is configured. The output power level of the final channel selected by DFS scan can be found in the Event Log.*

The Dynamic Frequency Selection (DFS) feature is enabled automatically when you choose a country with a regulatory domain that requires it. The Transmit Power Control (TPC) feature is always available.

Click the **Configure** button and the **System** tab; then select the appropriate country for your regulatory domain from the **Country** drop-down box.

Continue configuring settings as desired; then click the **Commands** button and the **Reboot** tab to save and activate the settings. Alternatively, if you want to save the configuration settings to the flash memory but not activate the settings, use the **save config** CLI command.

Dynamic Frequency Selection (DFS)

The Tsunami MP.11 5054-R supports Dynamic Frequency Selection (DFS) for European Telecommunications Standard Institute (ETSI) domains per EN 301-893 regulations. The ETSI requires that 802.11a devices use DFS to prevent interference with radar systems and other devices that already occupy the 5 GHz band.

During boot-up, the unit scans the available frequency and selects a channel that is quiet and free of radar interference. If the unit subsequently detects radar interference on its channel, it rescans to find a better channel. Upon finding a new channel, the unit waits 60 seconds to detect radar interference; if it finds no interference, it switches to the new channel.

If you are using a 5054-R unit in Europe or other applicable countries, keep in mind the following:

- DFS is not a configurable parameter; it is always enabled and cannot be disabled.
- You cannot manually select the device’s operating channel; you must let the unit select the channel. However, you can specify a particular “preferred” channel that you want to scan first whenever the DFS process starts. You may also make channels unavailable by manually “blacklist” them and prevent those channels to be scanned, as well as display the Channel Blacklist Table.
- You cannot configure the **Auto Channel Select** option. Within the HTTP or CLI interface, this option always appears enabled.

With 5054-R units, Dynamic Frequency Selection (DFS) is enabled automatically based upon the country you select. You can tell DFS is in use because the frequency selection field displays only the DFS-selected frequency. DFS scans all available frequencies, starting with the DFS preferred channel and skipping blacklisted channels, to select the operating frequency automatically.

A country selection with DFS enabled causes the Base Station to come up in scan mode. It scans the available frequencies and channels to avoid radar and selects a channel with the least interference.

NOTE: *Scanning is performed only on the frequencies allowed in the regulatory domain of the country selected when it is required for radar detection and avoidance.*

To comply with your country’s regulations, change the DFS selection to specify your country. You can do this by logging into the unit, clicking the **Configure** button and selecting the **System** tab. There is a drop-down box labeled **Country** with all available countries from which to select. Choose your country, configure the unit as required, and reboot for the settings to take effect.

The SU also comes up in scan mode to scan all available frequencies to find a BSU with which it can register. Scanning may take several minutes. After establishing a wireless link, the wireless LED stops flashing and continues to shine green.

NOTE: *Because DFS may need to scan for radar on multiple channels, you must allow a sufficient amount of time for the units to start up. This is considerably longer than when the unit is not using DFS. This is expected behavior. Startup time is within four minutes if no radar is detected, but up to one minute is added for every selected channel that results in radar detection.*

DFS is required for two purposes:

1. *Radar avoidance both at startup and while operational*. To meet these requirements, the BSU scans available frequencies at startup for the presence of a radar signal on all available frequencies. If a radar signal is detected on any DFS enabled channel, the system will blacklist the channel for a period of 30 minutes in accordance to EN301-

893. Once fully operational on a frequency, the BSU actively monitors the occupied frequency for radar interference. If radar interference is detected, the BSU blacklists the channel, logs a message and rescans to find a new frequency free of radar interference.

Radar detection is performed only by the BSU and not by the SU. When an SU is set to a country in which DFS is used, it scans all available channels upon startup looking for a BSU that best matches its connection criteria (such as **Base Station System Name**, **Network Name**, and **Shared Secret**). The SU connects to the BSU automatically on whatever frequency the BSU has selected. Because of this procedure, it is best to set up the BSU and have it fully operational before installing the SU, although this is not required. If a BSU rescans because of radar interference, the SU loses its wireless link. The SU waits 30 seconds (when the Mobility feature is enabled, the SU starts scanning for a BSU instantly rather than waiting 30 seconds); if it finds that it could not receive the BSU in this amount of time, it rescans the available frequencies for an active BSU.

2. *Guarantee the efficient use of available frequencies by all devices in a certain area*. To meet this requirement, the BSU scans each available frequency upon startup and selects a frequency based upon the least amount of noise and interference detected. This lets multiple devices operate in the same area with limited interference. This procedure is done only at startup; if another non-radar device comes up on the same frequency, the BSU does not detect this or rescan because of it. It is expected that other devices using these frequencies also are in compliance with country regulations, so this should not happen.

Transmit Power Control

Transmit Power Control is a manual configuration selection to reduce the unit’s output power. The maximum output power level for the operating frequency can be found in the event log of the unit’s embedded software.

By default, the unit lets you transmit at the maximum output power that the radio can sustain for data rate and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country. Also, most countries in the ETSI regulatory domain require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits, as part of the DFS requirements.

You can see your unit’s current output power for the selected frequency in the event log. The event log shows the selected power for all data rates, so you must look up the relevant data rate to determine the actual power level.

NOTE: *This feature only lets you decrease your output power; you cannot increase your output power beyond the maximum the radio allows for your frequency and data rate.*

See System Status to configure **Country.** See Configure the Wireless Interface to configure Transmit Power Control.

SU Registration

The list of parameters you must configure for registration of the SU on a BSU are:

- Network Name
- Base Station System Name (when used; otherwise, leave blank)
- Network Secret
- Encryption (when used)
- Frequency Channel (or Roaming, or DFS)

See System Parameters to see the description of these fields and to configure them.

NOTES:

- *The frequency channel must be the same for the BSU and the SU in order to register the SU when roaming is not enabled and DFS is not required.*
- *Channel Bandwidth and Turbo mode must be the same for the BSU and SU in order to register the SU.*
- *Roaming will automatically select a channel on the SU corresponding to the BSU channel. Roaming is the procedure in which an SU terminates the session with the current BSU and starts the registration procedure with another BSU when it finds the quality of the other BSU to be better.*

Dynamic Data Rate Selection (DDRS)

The WORP Dynamic Data Rate Selection (DDRS) lets the BSU and SUs monitor and calculate the remote average signal-to-noise ratio (SNR) and adjust the transmission data rate to an optimal value to provide the best possible throughput according to the current communication conditions and link quality during run-time.

Each frame received in the WORP protocol reports the signal and noise level in dBm at which the sender received the previous frame from the receiver, and provides the values to calculate the SNR in dB. SNR is calculated according to this formula then averaged:

SNR [dB] = signal level [dBm] – noise level [dBm]

Both the BSU and the SUs monitor the remote SNR. The BSU monitors and calculates the average remote SNR for each SU that is registered. An SU monitors and calculates the average remote SNR for the BSU.

DDRS is enabled or disabled on the BSU only. This operation requires the BSU to be rebooted. After rebooting, the BSU sends a multicast announcement to all SUs to begin the registration process. During registration, an SU is informed by the BSU whether DDRS is enabled or disabled and it sets its DDRS status accordingly.

There are two DDRS data rates that need to be configured when DDRS is enabled:

- **Default DDRS Data Rate** (*ddrsdefdatarate*): The data rate at which the BSU starts communication with all SUs to begin the registration process (the default is 6 Mbps).
- **Maximum DDRS Data Rate** (*ddrsmaxdatarate*): The maximum data rate at which the device (BSU or SU) can operate (the default is 54 Mbps).

NOTE: *The default (BSU only) and maximum (BSU and SU) DDRS data rate values must be configured in the BSU and SUs separately through the CLI or the SNMP interface.*

Virtual Local Area Networks (VLANs)

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to connected hosts) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify allowing traffic to flow between hosts and their frequently-used or restricted resources according to the VLAN configuration.

Tsunami MP.11 5054-R and 2454-R units are fully VLAN-ready; however, by default, VLAN support is disabled. Before enabling VLAN support (by assigning a VLAN Management ID), certain network settings should be configured and network resources such as VLAN-aware switches should be available, dependent upon the type of configuration.

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage VLAN configuration from a single window
- Define groups
- Reduce broadcast and multicast traffic to unnecessary destinations
  - Improve network performance and reduce latency
- Increase security
  - Secure network restricts members to resources on their own VLAN

VLAN tagged data is collected and distributed through a unit’s Ethernet interface. The units can communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports when the units are working in their Transparent mode.

VLAN features can be managed via:

- The BSU’s Web interface
- The Command Line Interface (see “Command Line Interface” in the *Reference Manual*)
- SNMP (see the MIBs provided on the product CD)

For more information about VLAN configuration, see VLAN Parameters.

Quality of Service (QoS)

The Quality of Service (QoS) feature is based on the 802.16 standard and defines the classes, service flows, and packet identification rules for specific types of traffic. QoS main priority is to guarantee a reliable and adequate transmission quality for all types of traffic under conditions of high congestion and bandwidth over-subscription.

Concepts and Definitions

The software supports QoS provisioning from the BSU only. You may define different classes of service on a BSU that can then be assigned to the SUs that are associated, or that may get associated, with that BSU.

The software provides the ability to create, edit, and delete classes of service that are specified by the following hierarchy of parameters:

- Packet Identification Rule (PIR) – up to 64 rules, including 17 predefined rules
- Service Flow class (SFC) – up to 32 SFs, including 7 predefined SFCs; up to 8 PIRs may be associated per SFC
- Priority for each rule within each SF class – 0 to 255, with 0 being lowest priority
- QoS class – up to 8 QoS classes, including 4 predefined classes; up to 4 SFCs may be associated per QoS class

Packet Identification Rule (PIR)

A Packet Identification Rule is a combination of parameters that specifies what type of traffic is allowed or disallowed. The software allows to create up to 64 different PIRs, including 17 predefined PIRs. It provides the ability to create, edit, and delete PIRs that contain none, one, or more of the following classification fields:

- Rule Name
- IP ToS (Layer 3 QoS identification)
- IP Protocol List containing up to 4 IP protocols
- 802.1p tag (layer 2 QoS identification)
- Up to 4 pairs of Source IP address + Mask
- Up to 4 pairs of Destination IP address + Mask
- Up to 4 source TCP/UDP port ranges
- Up to 4 destination TCP/UDP port ranges
- Up to 4 source MAC addresses
- Up to 4 destination MAC addresses
- VLAN ID
- Ether type (Ethernet protocol identification)

A good example is provided by the 17 predefined PIRs. Note that these rules help to identify specific traffic types:

1. All – No classification fields, all traffic matches
2. Cisco VoIP UL
   a. Protocol Source Port Range (16,000-32,000)
   b. IP Protocol List (17 = UDP)
3. Vonage VoIP UL
   a. Protocol Source Port Range (8000-8001, 10000-20000)
   b. IP Protocol List (17 = UDP)
4. Cisco VoIP DL
   a. Protocol Destination Port Range (16,000-32,000)
   b. IP Protocol List (17 = UDP)
5. Vonage VoIP DL

   a. Protocol Destination Port Range (8000-8001, 10000-20000)
   b. IP Protocol List (17 = UDP)

6. TCP
   a. IP Protocol List (6)
7. UDP
   a. IP Protocol List (17)
8. PPPoE Control
   a. Ethertype (type 1, 0x8863)
9. PPPoE Data
   a. Ethertype (type 1, 0x8864)
10. IP
   a. Ethertype (type 1, 0x800)
11. ARP
   a. Ethertype (type 1, 0x806)
12. Expedited Forwarding
   a. IP TOS/DSCP (low=0x2D, high=0x2D, mask = 0x3F)
13. Streaming Video (IP/TV)
   a. IP TOS/DSCP (low=0x0D, high=0x0D, mask = 0x3F)
14. 802.1p BE
   a. Ethernet Priority (low=0, high=0) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
15. 802.1p Voice
   a. Ethernet Priority (low=6, high=6) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
16. 802.1p Video
   a. Ethernet Priority (low=5, high=5) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
17. L2 Broadcast/Multicast
   a. Ethernet Destination (dest = 0x80000000, mask = 0x80000000)

Two different VoIP rule names have been defined for each direction of traffic, Uplink (UL) and Downlink (DL), (index numbers 2 to 5). This has been done to distinguish the proprietary nature of the Cisco VoIP implementation as opposed to the more standard Session Initiation Protocol (SIP) signaling found, for example, in the Vonage-type VoIP service.

Service Flow Class (SFC)

A Service Flow class defines a set of parameters that determines how a stream of application data that matches a certain classification profile will be handled. The software allows to create up to 32 different SFs, including seven predefined SFs. The software provides the ability to create, edit, and delete SFs that contain the following parameters and values:

- Service flow name
- Scheduling type – Best Effort (BE); Real-Time Polling Service (RtPS)
- Service Flow Direction – Downlink (DL: traffic from BSU to SU); Uplink (UL: traffic from SU to BSU)
- Maximum sustained data rate (or Maximum Information Rate, MIR) – specified in units of 1 Kbps from 8 Kbps up to he maximum rate of 108000 Kbps per SU
- Minimum reserved traffic rate (or Committed Information Rate, CIR) – specified in units of 1 Kbps from 0 Kbps up to the maximum rate of 10000 Kbps per SU

- Maximum Latency – specified in increments of 5 ms steps from a minimum of 5 ms up to a maximum of 100 ms
- Tolerable Jitter – specified in increments of 5 ms steps from a minimum of 0 ms up to the Maximum Latency (in ms)
- Traffic priority – zero (0) to seven (7), 0 being the lowest, 7 being the highest
- Maximum number of data messages in a burst – one (1) to four (4), which affects the percentage of the maximum throughput of the system
- Activation state – Active; Inactive

Note that traffic priority refers to the prioritization of this specific Service Flow.

The software tries to deliver the packets within the specified latency and jitter requirements, relative to the moment of receiving the packets in the unit. For delay-sensitive traffic the jitter must be equal to or less than the latency. A packet is buffered until an interval of time equal to the difference between Latency and Jitter (Latency – Jitter) has elapsed. The software will attempt to deliver the packet within a time window starting at (Latency – Jitter) until the maximum Latency time is reached. If the SFC's scheduling type is real-time polling (rtPS), and the packet is not delivered by that time, it will be discarded. This can lead to loss of packets without reaching the maximum throughput of the wireless link. For example, when the packets arrive in bursts on the Ethernet interface and the wireless interface is momentarily maxed out, then the packets at the "end" of the burst may be timed out before they can be sent.

Users are able to set up their own traffic characteristics (MIR, CIR, latency, jitter, etc.) per service flow class to meet their unique requirements. A good example is provided by the seven predefined SFCs:

1. UL-Unlimited BE
   a. Scheduling Type = Best Effort
   b. Service Flow Direction = Uplink
   c. Initialization State = Active
   d. Maximum Sustained Data Rate = 20 Mbps
   e. Traffic Priority = 0
2. DL-Unlimited BE (same as UL-Unlimited BE, except Service Flow Direction = Downlink)
3. UL-G711 20 ms VoIP rtPS
   a. Schedule type = Real time Polling
   b. Service Flow Direction = Uplink
   c. Initialization State = Active
   d. Maximum Sustained Data Rate = 88 Kbps
   e. Minimum Reserved Traffic Rate = 88 Kbps
   f. Maximum Latency = 20 milliseconds
   g. Traffic Priority = 1
4. DL-G711 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Service Flow Direction = Downlink)
5. UL-G729 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Maximum Sustained Data Rate and Maximum Reserved Traffic Rate = 64 Kbps)
6. DL-G729 20 ms VoIP rtPS (same as UL-G729 20ms VoIP rtPS, except Service Flow Direction = Downlink)
7. DL-2Mbps Video
   a. Schedule type = Real time Polling
   b. Service Flow Direction = Downlink
   c. Initialization State = Active
   d. Maximum Sustained Data Rate = 2 Mbps
   e. Minimum Reserved Traffic Rate = 2 Mbps
   f. Maximum Latency = 20 milliseconds
   g. Traffic Priority = 1

Two different VoIP Service Flow classes for each direction of traffic have been defined (index numbers 3 to 6) which follow the ITU-T standard nomenclatures: G.711 refers to a type of audio companding and encoding that produces a 64 Kbps bitstream, suitable for all types of audio signals. G.729 is appropriate for voice and VoIP applications, but cannot transport music or fax tones reliably. This type of companding and encoding produces a bitstream between 6.4 and 11.8 Kbps (typically 8 Kbps) according to the quality of voice transport that is desired.

QoS Class

A QoS class is defined by a set of parameters that includes the PIRs and SFCs that were previously configured. The software allows creating up to eight different QoS classes, including four predefined QoS classes. Up to four SF classes can be associated to each QoS class, and up to eight PIRs can be associated to each SF class. For example, a QoS class called “G711 VoIP” may include the following SFCs: “UL-G711 20 ms VoIP rtPS” and “DL-G711 20 ms VoIP rtPS”. In turn, the SFC named “UL-G711 20 ms VoIP rtPS” may include the following rules: “Cisco VoIP UL” and “Vonage VoIP UL”.

The software provides the ability to create, edit, and delete QoS classes that contain the following parameters:

- QoS class name
- Service Flow (SF) class name list per QoS class (up to four SF classes can be associated to each QoS class)
- Packet Identification Rule (PIR) list per SF class (up to eight PIRs can be associated to each SF class)
- Priority per rule which defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.

A good example of this hierarchy is provided by the four predefined QoS classes:

1. Unlimited Best Effort
   a. SF class: UL-Unlimited BE
      PIR: All; PIR Priority: 0
   b. SF class: DL-Unlimited BE
      PIR: All; PIR Priority: 0
2. G711 VoIP
   a. SF class: UL-G711 20 ms VoIP rtPS
      PIR: Vonage VoIP UL; PIR Priority: 1
      PIR: Cisco VoIP UL; PIR Priority: 1
   b. SF class: DL-G711 20 ms VoIP rtPS
      PIR: Vonage VoIP DL; PIR Priority: 1
      PIR: Cisco VoIP DL; PIR Priority: 1
3. G729 VoIP
   a. SF class: UL-G729 20 ms VoIP rtPS
      PIR: Vonage VoIP UL; PIR Priority: 1
      PIR: Cisco VoIP UL; PIR Priority: 1
   b. SF class: DL-G729 20 ms VoIP rtPS
      PIR: Vonage VoIP DL; PIR Priority: 1
      PIR: Cisco VoIP DL; PIR Priority: 1
4. 2Mbps Video
   a. SF class: DL-2Mbps Video
      PIR: Streaming Video (IP/TV); PIR Priority: 1

Basic Management

4

This chapter describes basic features and functionality of the unit. In most cases, configuring these basic features is sufficient. The “Glossary” in the *Tsunami MP.11 Reference Manual* provides a brief explanation of the terms used. For CLI commands you can use for basic management, see “Command Line Interface” in the *Tsunami MP.11 Reference Manual*.

The following topics are discussed in this chapter:

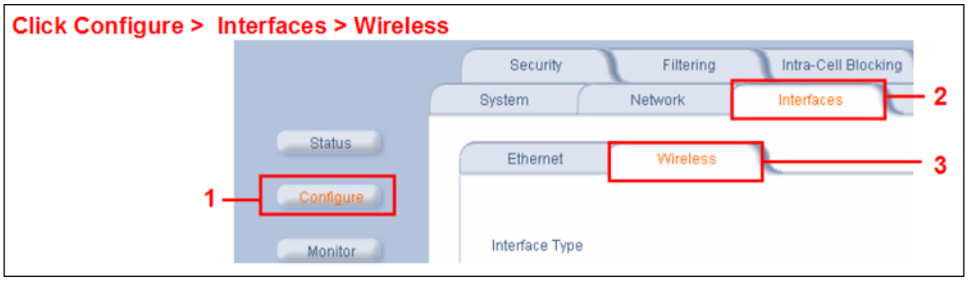
- Navigation
- Rebooting and Resetting
- General Configuration Settings
- Monitoring Settings
- Security Settings
- Default Settings
- Upgrading the Unit

Navigation

To use the Web Interface for configuration and management, you must access the unit. With ScanTool you can determine the unit’s current IP address. Then enter **http://<ip address>** in your Web browser (for example **http://10.0.0.1**). See Setting the IP Address with ScanTool for details.

NOTE: *If you have your Security Internet Options set to **High**, you may not be able to access the Web interface successfully; a high security setting disables JavaScript, which is required for running Proxim’s Web browser interface. Adding the radio’s IP address as a Trusted site should fix this problem.*

The Web Interface consists of Web page buttons and tabs. A tab can also contain sub-tabs. The following figure shows the convention used to guide you to the correct tab or sub-tab.



The Web Interface also provides online help, which is stored on your computer (see Step 9: Install Documentation and Software for details).

Rebooting and Resetting

All configuration changes require a restart unless otherwise stated. You can restart the unit with the **Reboot** command; see Rebooting, below).

Most changes you make become effective only when the unit is rebooted. A reboot stores configuration information in non-volatile memory and then restarts the unit with the new values (see Soft Reset to Factory Default).

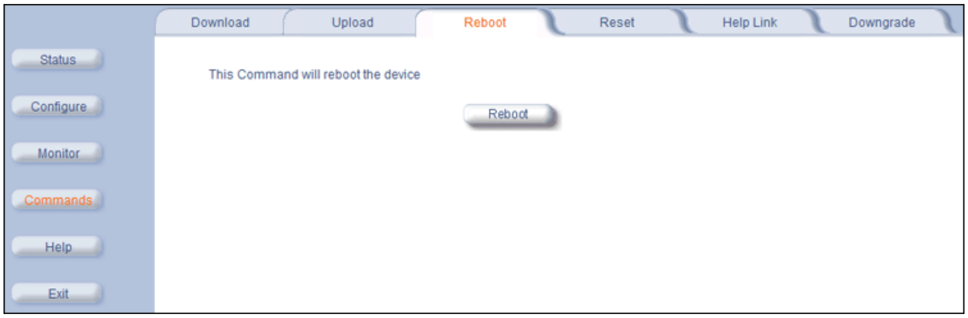
In some cases, the unit reminds you that a reboot is required for a change to take effect. You need not reboot immediately; you can reboot after you have made all your changes.

NOTE: *Saving of the unit's configuration occurs only during a controlled reboot or by specifically issuing the CLI **Save** command. If you make changes to settings without a controlled reboot (command) and you have not issued the **Save** command, a power outage would wipe out all changes since the last reboot. For example, entering static routes takes effect immediately; however, the routes are not saved until the unit has gone through a controlled reboot. Proxim strongly recommends saving your settings immediately when you finish making changes.*

Rebooting

When you reboot, the changes you have made become effective and the unit is restarted. The changes are saved automatically in non-volatile memory before the actual reboot takes place.

To reboot, click **Commands** > **Reboot** > **Reboot**. The unit restarts the embedded software. During reboot, you are redirected to a page showing a countdown timer, and you are redirected to the **Status** page after the timer counts down to 0 (zero). The CLI is disconnected during reboot. This means that a new telnet session must be started.


This Command will reboot the device

Resetting Hardware

If the unit does not respond for some reason and you are not able to reboot, you can restart by means of a hardware reset. This restarts the hardware and embedded software. The last saved configuration is used. Any changes that you have made since then are lost.

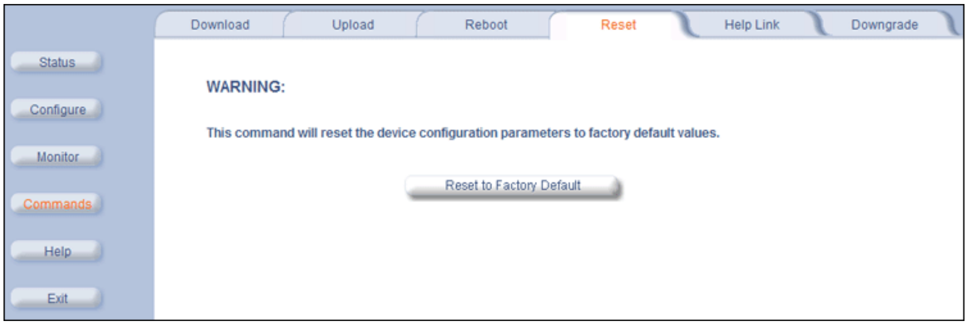
To reset the hardware, unplug the unit's power supply and then reconnect power to the unit.

Soft Reset to Factory Default

If necessary, you can reset the unit to the factory default settings. *This should be done only when you are experiencing problems*. Resetting to the default settings requires you to reconfigure the unit.

To reset to factory default settings:

1. Click **Commands** > **Reset**.
2. Click the **Reset to Factory Default** button. The device configuration parameter values are reset to their factory default values.



WARNING:

This command will reset the device configuration parameters to factory default values.

If you do not have access to the unit, you can use the procedure described in Hard Reset to Factory Default as an alternative.

General Configuration Settings

- **System Status:** The Status tab showing the system status is displayed automatically when you log into the Web interface. It is also the default window displayed when you click the **Status** button on the left side of the window. See System Status for more information.
- **System Configuration:** The System Configuration window lets you change the unit's c*ountry*, *system name*, *location name*, and so on (see the window to the right). The Country selection is required to enable the correct radio parameters. The other details help distinguish this unit from other routers, and let you know whom to contact in case of problems. See System Parameters for more information.
- **IP Configuration:** The **IP Configuration** window lets you change the unit's IP parameters. These settings differ between **Routing** and **Bridge** mode. See Network Parameters for more information.
- **Interface Configuration:** The **Interface** configuration pages let you change the Ethernet and Wireless parameters. The **Wireless** tab is displayed by default when you click the **Interfaces** tab.
  - **Ethernet:** To configure the **Ethernet** interface, click **Configure** > **Interfaces** > **Ethernet**. You can set the **Configuration** parameter from this tab for the type of Ethernet transmission. The recommended setting is **auto-speed auto-duplex**. See Configure the Ethernet Interface for more information.
  - **Wireless:** To configure the **wireless** interface, click **Configure** > **Interfaces** > **Wireless**. For BSUs, the wireless interface can be placed in either **WORP Base** or **WORP Satellite** mode (selected from the **Interface Type** drop-down box). SUs can be placed only in **WORP Satellite** mode. (See Interface Parameters for more information.)
- **VLAN Configuration:** To configure BSU VLAN parameters, click the **Configure** button followed by the **VLAN** tab; the **BSU Table** tab is displayed. Click the **SUs' Table** tab to configure SU VLAN parameters. Virtual LAN (VLAN) implementation in the Tsunami MP.11 products lets the BSU and SU be used in a VLAN-aware network and processes IEEE 802.1Q VLAN-tagged packets. Network resources behind the BSU and SU can be assigned to logical groups. See VLAN Parameters for more information.

Monitoring Settings

The unit offers various facilities to monitor its operation and interfaces. Only the most significant monitoring categories are mentioned here.

- **Wireless:** To monitor the wireless interfaces, click **Monitor** > **Wireless**. This tab lets you monitor the general performance of the radio and the performance of the **WORP Base** or **WORP Satellite** interfaces.
- **Interfaces:** To monitor transmission details, click **Monitor** > **Interfaces**. The **Interfaces** tab provides detailed information about the MAC-layer performance of the wireless network and Ethernet interfaces.
- **Per Station:** Click **Monitor** > **Per Station** to view **Station Statistics**. On the SU, the **Per Station** page shows statistics of the BSU to which the SU is registered. On the BSU, it shows statistics of all the SU's connected to the BSU. The page's statistics refresh every 4 seconds.

Security Settings

To prevent misuse, the 5054-R and 2454-R provide wireless data encryption and password-protected access. *Be sure to set the encryption parameters and change the default passwords.*

In addition to Wired Equivalent Privacy (WEP), the units support Advanced Encryption Standard (AES) 128-bit encryption. Two types of the AES encryption are available. Previous releases supported only the AEC-OCB; the AES CCM protocol is now also supported.

Proxim highly recommends you change the **Network Name**, **Encryption Key**, and **Shared Secret** as soon as possible. To do so, click **Configure** > **Interfaces > Wireless**. The encryption key is set using the **Security** tab. For systems that will use roaming features, the **Network Name**, **Encryption Key**, and the **Shared Secret** should each be the same for all SUs that are allowed to roam as well as for all BSUs to which these SUs are allowed to roam.

Encryption

You can protect the wireless data link by using encryption. Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values.

To set the encryption parameters, click **Configure** > **Security** > **Encryption**. See Configure Encryption Parameters.

Passwords

Access to the units are protected with passwords. The default password is **public**. For better security it is recommended to change the default passwords to a value (6-32 characters) known only to you.

To change the unit's HTTP, Telnet, or SNMP passwords, click **Configure** > **Management** > **Password**. See Configure Passwords.

Default Settings

Feature	Model	
	5054-R	2454-R
System Name	Tsunami MP.11 5054-R	Tsunami MP.11 2454-R
Mode of Operation	Bridge	Bridge
Routing	Disabled	Disabled
IP Address Assignment Type	Static	Static
IP Address	10.0.0.1	10.0.0.1
Subnet Mask	255.255.255.0	255.255.255.0
Default Router IP Address	10.0.0.1	10.0.0.1
Default TTL	64	64
RIPv2	Enabled when in Routing Mode	Enabled when in Routing Mode
Base Station System Name	<blank>	<blank>
Network Name	OR_WORP	OR_WORP
Frequency Channel	Channel 149, Frequency 5.745 GHz (FCC Only devices) DFS Enabled (World Mode devices)	Channel 10 (2.412 – 2.462 GHz)
Transmit Power Control	0 dB	0 dB
Data Rate	36 Mbps	36 Mbps
Registration Timeout	5	5
Network Secret	public	public
Turbo Mode	Disabled	Not applicable
Channel Bandwidth	20 MHz	20 MHz
Input bandwidth limit (in Kbps)	36032	36032
Output bandwidth limit (in Kbps)	36032	36032
Ethernet Configuration	Auto-Speed Auto-Duplex	Auto-Speed Auto-Duplex
Serial port Baud Rate	9600	9600
SNMP Management Interface	Enabled	Enabled
Telnet Management Interface	Enabled	Enabled
HTTP Management Interface	Enabled	Enabled
HTTP Port	80	80
Telnet Port	23	23
Telnet Login Timeout	30	30
Telnet Session Timeout	900	900
Password	public	public
Maximum Satellites (per BSU)	250	250
MAC Authentication	Disabled	Disabled
Radius Authentication	Disabled	Disabled
Encryption	Disabled	Disabled
Static MAC Address Filter	Disabled / No Entries	Disabled / No Entries
Ethernet Protocol Filtering	All Filters Disabled	All Filters Disabled
DFS Priority Frequency Channel	Disabled	N/A
Announcement Period (when roaming enabled)	100 ms	100 ms

Feature	Model	
	5054-R	**2454-R**
Multi-Frame Bursting	Enabled	Enabled
Storm Threshold	Broadcast/Multicast Unlimited	Broadcast/Multicast Unlimited
Broadcast Protocol Filtering	All Protocols Allowed	All Protocols Allowed
Dynamic Data Rate Selection	Disabled	Disabled
Roaming	Disabled	Disabled
NAT	Disabled	Disabled
Intra-Cell Blocking	Disabled	Disabled
Antenna Alignment	Disabled	Disabled
Country Selection	US-only device – US World device – GB	US-only device – US World device – GB
DHCP Server	Disabled	Disabled
DHCP Relay	Disabled	Disabled
Spanning Tree Protocol	Disabled	Disabled
Antenna Gain (For DFS Threshold compensation)	0	0
Satellite Density	Large	Large
Temperature Logging	Enabled	Enabled
Temperature Logging Interval	60 minutes	60 minutes
VLAN Mode	BSU: Transparent Mode SU: Transparent mode when BSU in transparent mode; Trunk mode when BSU in Trunk mode	
Access VLAN ID	BSU: N/A; SU: 1	
Access VLAN Priority	BSU: N/A; SU: 0	
Management VLAN ID	BSU: -1; SU: -1	
Management VLAN Priority	BSU: 0; SU: 0	
VLAN ID in Trunk VLAN Table	BSU: N/A; SU: 1	

Upgrading the Unit

The units are equipped with embedded software that can be updated when new versions are released. Updating the embedded software is described in Web Interface Image File Download. A TFTP server is provided on the Documentation and Software CD; the server is required to transfer the downloaded file to the unit. See TFTP Server Setup.

To access all resolved problems in our solution database, or to search by product, category, keywords, or phrases, go to http://support.proxim.com. You can also find links to drivers, documentation, and downloads at this link.

5

System Status

This chapter describes viewing system status and event log information from the unit’s Web Interface.

Click on the **Status** button to access system and event log information. See the following sections:

- System Status
- Event Log

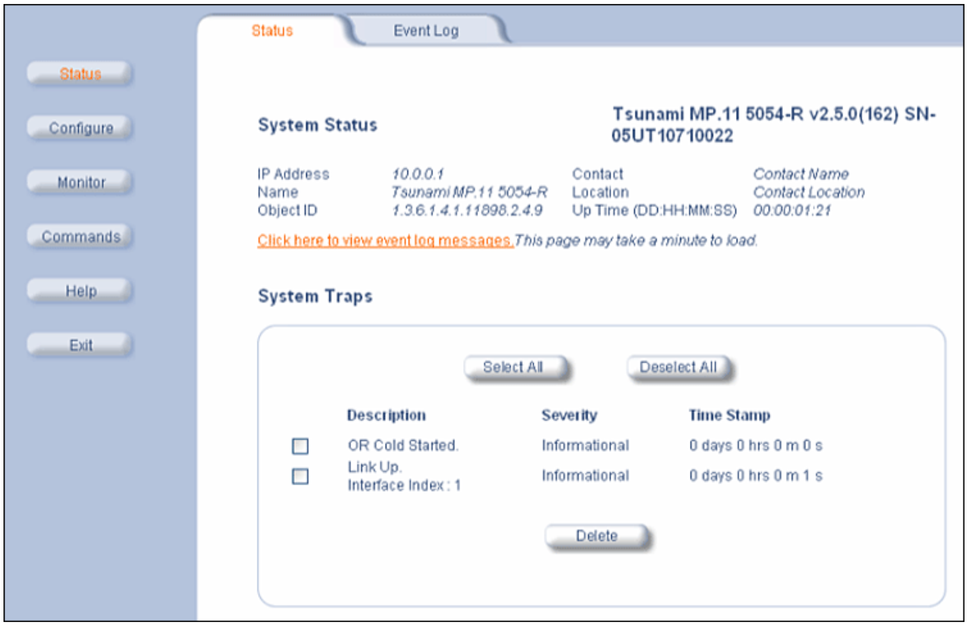
Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

System Status

The **Status** tab showing the system status is displayed automatically when you log into the Web Interface. It also is the default window displayed when you click the **Status** button on the left side of the window.

The **Status** tab shows the **System Status** and the **System Traps**.



System Status

Tsunami MP.11 5054-R v2.5.0(162) SN-05UT10710022

IP Address	*10.0.0.1*	Contact	*Contact Name*
Name	*Tsunami MP.11 5054-R*	Location	*Contact Location*
Object ID	*1.3.6.1.4.1.11898.2.4.9*	Up Time (DD:HH:MM:SS)	*00:00:01:21*

Click here to view event log messages. *This page may take a minute to load.*

System Traps

	Description	Severity	Time Stamp
□	OR Cold Started.	Informational	0 days 0 hrs 0 m 0 s
□	Link Up. Interface Index : 1	Informational	0 days 0 hrs 0 m 1 s

System Status

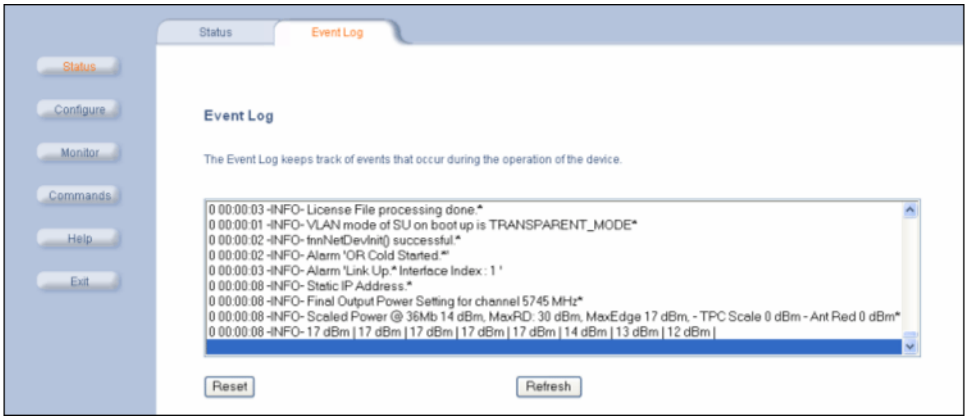
The basic system status is shown in this section, including the version number of the embedded software.

Systems Traps

The status of system traps is shown in this section. System traps occur when the unit encounters irregularities. Deleting system traps has no effect on the operation of the unit. System traps also are sent to an SNMP manager station (if so configured). See “Alarm Traps” in the *Tsunami MP.11 Reference Manual* for a list and description of the traps.

Event Log

Click the **Status** button and the **Event Log** tab to view the contents of your Event Log. The **Event Log** keeps track of events that occur during the operation of the unit. The **Event Log** displays messages that may not be captured by System Traps, such as the **Transmit Power** for the **Frequency Channel** selected.



Event Log

The Event Log keeps track of events that occur during the operation of the device.

```
0 00:00:03 -INFO- License File processing done.*
0 00:00:01 -INFO- VLAN mode of SU on boot up is TRANSPARENT_MODE*
0 00:00:02 -INFO- fnnNetDevInit() successful.*
0 00:00:02 -INFO- Alarm 'OR Cold Started.*'
0 00:00:03 -INFO- Alarm 'Link Up.* Interface Index : 1 '
0 00:00:08 -INFO- Static IP Address.*
0 00:00:08 -INFO- Final Output Power Setting for channel 5745 MHz*
0 00:00:08 -INFO- Scaled Power @ 36Mb 14 dBm, MaxRD: 30 dBm, MaxEdge 17 dBm, - TPC Scale 0 dBm - Ant Red 0 dBm*
0 00:00:08 -INFO- 17 dBm | 17 dBm | 17 dBm | 17 dBm | 17 dBm | 14 dBm | 13 dBm | 12 dBm |
```

See “Event Log Error Messages” in the *Tsunami MP.11 Reference Manual* for an explanation of messages that can appear in the Event Log.

Configuration

6

This chapter describes configuring the unit's settings using the unit's Web Interface.

Click the **Configure** button to access configuration settings.

The following topics are discussed in this section:

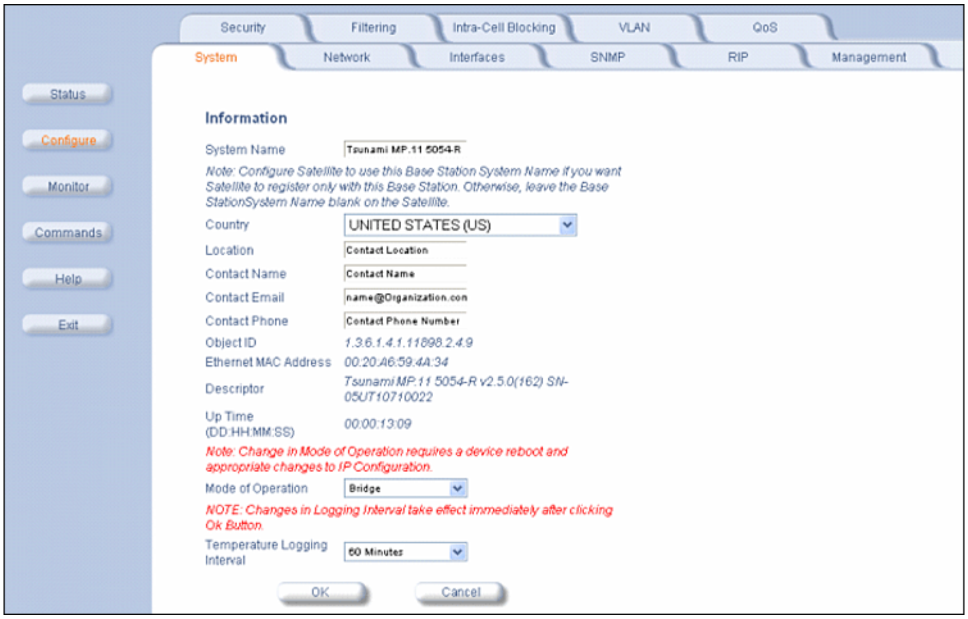
Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

System Parameters

The **System** configuration page lets you change the unit's **System Name**, **Location**, **Mode of Operation**, and so on. These details help you to distinguish the unit from other routers and let you know whom to contact in case you experience problems.

Click the **Configure** button and the **System** tab; the following window is displayed.



Information

System Name: Tsunami MP.11 5054-R

Note: Configure Satellite to use this Base Station System Name if you want Satellite to register only with this Base Station. Otherwise, leave the Base StationSystem Name blank on the Satellite.

Country: UNITED STATES (US)

Location: Contact Location

Contact Name: Contact Name

Contact Email: name@Organization.con

Contact Phone: Contact Phone Number

Object ID: *1.3.6.1.4.1.11898.2.4.9*

Ethernet MAC Address: *00:20:A6:59:4A:34*

Descriptor: *Tsunami MP.11 5054-R v2.5.0(162) SN-05UT10710022*

Up Time (DD:HH:MM:SS): *00:00:13:09*

Note: Change in Mode of Operation requires a device reboot and appropriate changes to IP Configuration.

Mode of Operation: Bridge

NOTE: Changes in Logging Interval take effect immediately after clicking Ok Button.

Temperature Logging Interval: 60 Minutes

You can enter the following details:

- **System Name:** This is the system name for easy identification of the BSU or SU. The System Name field is limited to a length of 32 bytes. Use the system name of a BSU to configure the Base Station System Name parameter on an SU if you want the SU to register only with this BSU. If the Base Station System Name is left blank on the SU, it can register with any Base Station that has a matching Network Name and Network Secret.
- **Country:** The Dynamic Frequency Selection (DFS) is enabled automatically when you choose a country with a regulatory domain that requires it. The Country selection pre-selects and displays only the allowed frequencies for the selected country.

  Click **Configure** > **Interfaces** > **Wireless** to see the channel/frequency list for the selected Country.

  NOTE: *Units sold in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other Country selections, channels, or frequencies can be configured. Units sold outside of the United States and Canada support the selection of a Country by the professional installer. If you change the Country, a reboot of the unit is necessary for the upgrade to take place.*

  Dynamic Frequency Selection is not supported in 2.4 GHz operational mode; it is supported on Model 5054-R units only.

  Support for the 5.25 – 5.35 GHz and 5.725 – 5.825 GHz frequency bands is provided with a single country selection, **UNITED STATES (US)**, which does not provide DFS capability in these frequency bands.

  For a non US-only device, the default country selected is **United Kingdom (GB)**.

  Note the following:

  – The channel center frequencies are not regulated; only the band edge frequencies are regulated.

  – If, before upgrade, US was selected as a country for a non US-Only device (which is an incorrect configuration), the country is changed automatically to United Kingdom upon upgrade.

  See Country Codes and Channels for a list of country codes.
- **Location:** This field can be used to describe the location of the unit, for example “Main Lobby.”
- **Contact Name**, **Contact Email**, and **Contact Phone:** In these fields, you can enter the details of the person to contact.
- **Mode of Operation:** This field sets the unit as **bridge** (layer 2) or as **router** (layer 3). See Bridge and Routing Modes for more information.

The static fields on this window are described as follows:

- **ObjectID:** This field shows the OID of the product name in the MIB.
- **Ethernet MAC Address:** The MAC address of the Ethernet interface of the device.
- **Descriptor:** Shows the product name and firmware build version.
- **Up Time:** The length of time the device has been up and running since the last reboot.

Bridge and Routing Modes

Bridge Mode

A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street. A bridge examines each message on a LAN, passing those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

In bridging networks, computer or node addresses have no specific relationship to location. For this reason, messages are sent out to every address on the network and accepted only by the intended destination node. Bridges learn which addresses are on which network and develop a learning table so that subsequent messages can be forwarded to the correct network.

Bridging networks are generally always interconnected LANs since broadcasting every message to all possible destination would flood a larger network with unnecessary traffic. For this reason, router networks such as the Internet use a scheme that assigns addresses to nodes so that a message or packet can be forwarded only in one general direction rather than forwarded in all directions.

A bridge works at the data-link (physical) layer of a network, copying a data packet from one network to the next network along the communications path.

The default Bridging Mode is **Transparent Bridging**.

This mode works if you do not use source routing in your network. If your network is configured to use source routing, then you should use either Multi-Ring SRTB or Single-Ring SRTB mode.

In Multi-Ring SRTB mode, each unit must be configured with the Bridge number, Radio Ring number, and Token Ring number. The Radio Ring number is unique for each Token Ring Access Point and the Bridge number is unique for each Token Ring Access Point on the same Token Ring segment.

Alternatively, you may use the Single-Ring SRTB mode. In this mode, only the Token Ring number is required for configuration.

Routing Mode

Routing mode can be used by customers seeking to segment their outdoor wireless network using routers instead of keeping a transparent or bridged network. By default the unit is configured as a bridge device, which means traffic between different outdoor locations can be seen from any point on the network.

By switching to routing mode, your network now is segmented by a layer 3 (IP) device. By using Routing mode, each network behind the BSU and SUs can be considered a separate network with access to each controlled through routing tables.

The use of a router on your network also blocks the retransmission of broadcast and multicast packets on your networks, which can help to improve the performance on your outdoor network in larger installations.

The use of Routing mode requires more attention to the configuration of the unit and thorough planning of the network topology of your outdoor network. The unit can use Routing mode in any combination of BSU and SUs. For example, you may have the BSU in Routing mode and the SU in Bridge mode, or vice versa.

When using Routing mode, pay close attention to the configuration of the default gateway both on your unit and on your PCs and servers. The default gateway controls where packets with unknown destinations (Internet) should be sent. Be sure that each device is configured with the correct default gateway for the next hop router. Usually this is the next router on the way to your connection to the Internet. You can configure routes to other networks on your Intranet through the addition of static routes in your router's routing table.

Key Reasons to Use Routing Mode

One key reason why customers would use Routing mode is to implement virtual private networks (VPNs) or to let nodes behind two different SUs communicate with each other. Many customers do this same thing in Bridging mode by using secondary interfaces on the router at the BSU or virtual interfaces at the BSU in VLAN mode to avoid some of the drawbacks of IP Routing mode.

Routing mode prevents the transport of non-IP protocols, which may be desirable for Service Providers.

Routing mode is usually more efficient because Ethernet headers are not transported and non-IP traffic is blocked.

Benefits of using Routing Mode

- Enabling RIP makes the unit easier to manage for a Service Provider that uses RIP to dynamically manage routes. RIP is no longer very common for Service Providers or Enterprise customers and an implementation of a more popular routing protocol like OSPF would be desirable.
- Routing mode saves bandwidth by not transporting non-IP protocols users might have enabled, like NetBEUI or IPX/SPX, which eliminates the transmission of broadcasts and multicasts.
  - The MAC header is:
    - Destination MAC: 6 bytes
    - Source MAC: 6 bytes
    - Ethernet Type: 2 bytes

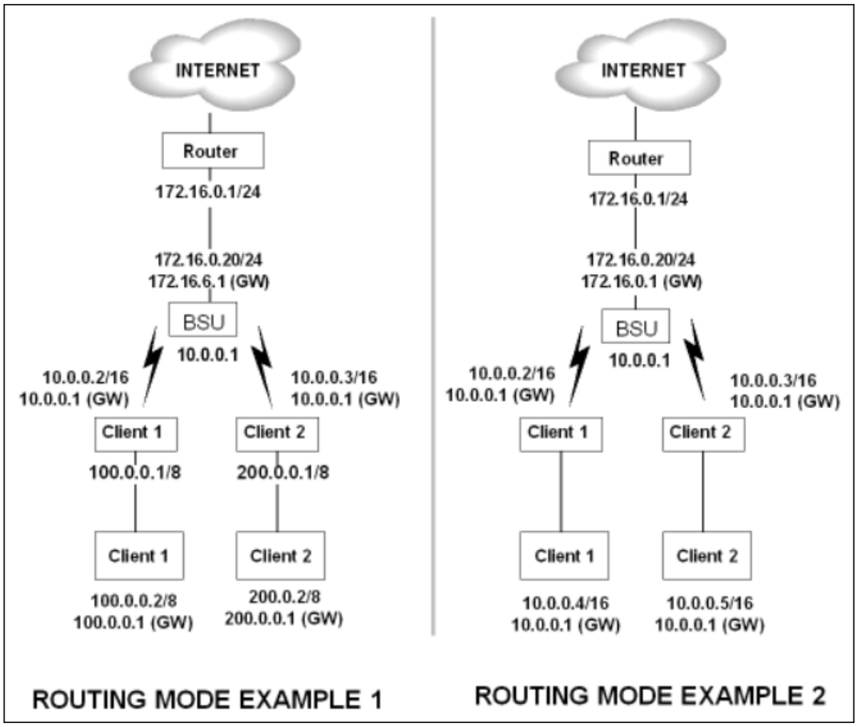
If the average packet size is 1000 bytes, the overhead saved is 1.5%; With a frame size of 64 bytes, the overhead saved is 20%; and for frame sizes of 128 bytes, the saving is 10%. Network researches claim that most network traffic consists of frames smaller than 100 bytes.

In order to support routers behind the SUs with multiple subnets and prevent routing loops, you want individual routes (and more than one) per SU.

Routing Mode Examples

In the first example, both the BSU and the SUs are configured for Routing mode. This example is appropriate for businesses connecting remote offices that have different networks.

In example 2, the BSU is in Routing mode and the SUs are in Bridge mode. Notice the PCs behind the SUs must configure their default gateways to point to the BSU, not the SU.



Notes:

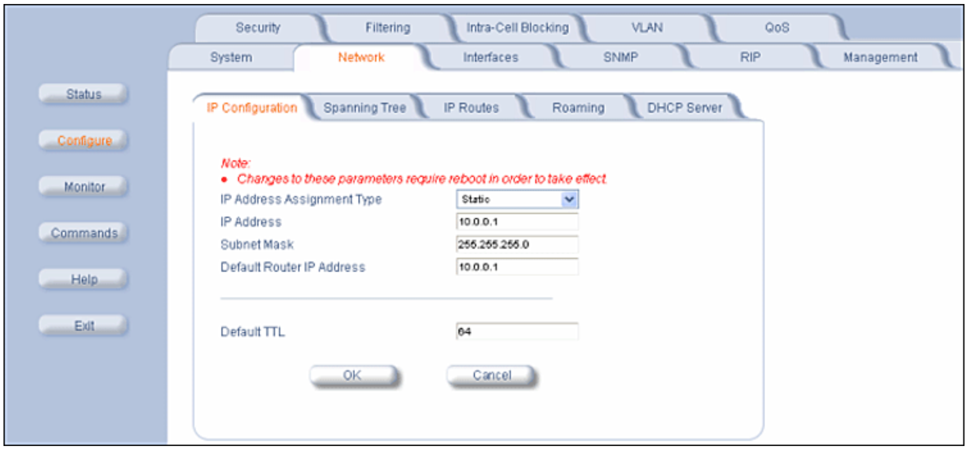
- One of the most important details to pay attention to in Routing mode are the unit's and the PC's default gateways. It is a common mistake to set up the PC's gateway to point to the SU when the SU is in Bridge mode and the BSU is in Routing mode. Always check to make sure the PCs on your network are configured to send their IP traffic to the correct default gateway.
- Be sure to reboot the unit to permanently save static routes. New routes take effect immediately without a reboot, but are not permanently saved with your configuration until you do reboot the device. An unexpected power outage could cause static routes you entered to "disappear" when the unit reboots if they have not been saved. You also should save a copy of your unit's configuration file in case the unit must be reloaded. This saves you from being required to re-enter numerous static routes in a large network.
- The routing table supports up to 500 static routes.

Network Parameters

Change IP Parameters

The IP Configuration window lets you change the IP parameters. These settings differ when the unit is in **Routing** mode.

Click **Configure** > **Network** > **IP Configuration** to view and configure local IP address information. See Setting the IP Address with ScanTool for more information.



Note:
- *Changes to these parameters require reboot in order to take effect*

IP Address Assignment Type: Static
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Default Router IP Address: 10.0.0.1

Default TTL: 64

If the device is configured in **Bridge** mode, you can set the **IP Address Assignment Type** parameter:

- Select ***Static*** if you want to assign a static IP address to the unit.
- Select ***Dynamic*** to have the device run in DHCP client mode, which gets an IP address automatically from a DHCP server over the network.

If you do not have a DHCP server or if you want to manually configure the IP settings, set this parameter to ***Static***.

When the unit is in **Bridge** mode, only one IP address is required. This IP address also can be changed with ScanTool (see Setting the IP Address with ScanTool). In **Routing** mode, both Ethernet and Wireless interfaces require an IP address.

You can set the following remaining parameters only when the **IP Address Assignment Type** is set to ***Static***.

- **IP Address:** The unit’s static IP address (default IP address is 10.0.0.1).
- **Subnet Mask:** The mask of the subnet to which the unit is connected (the default subnet mask is 255.255.255.0).
- **Default Router IP Address:** The IP address of the default gateway.
- **Default TTL:** The default time-to-live value.

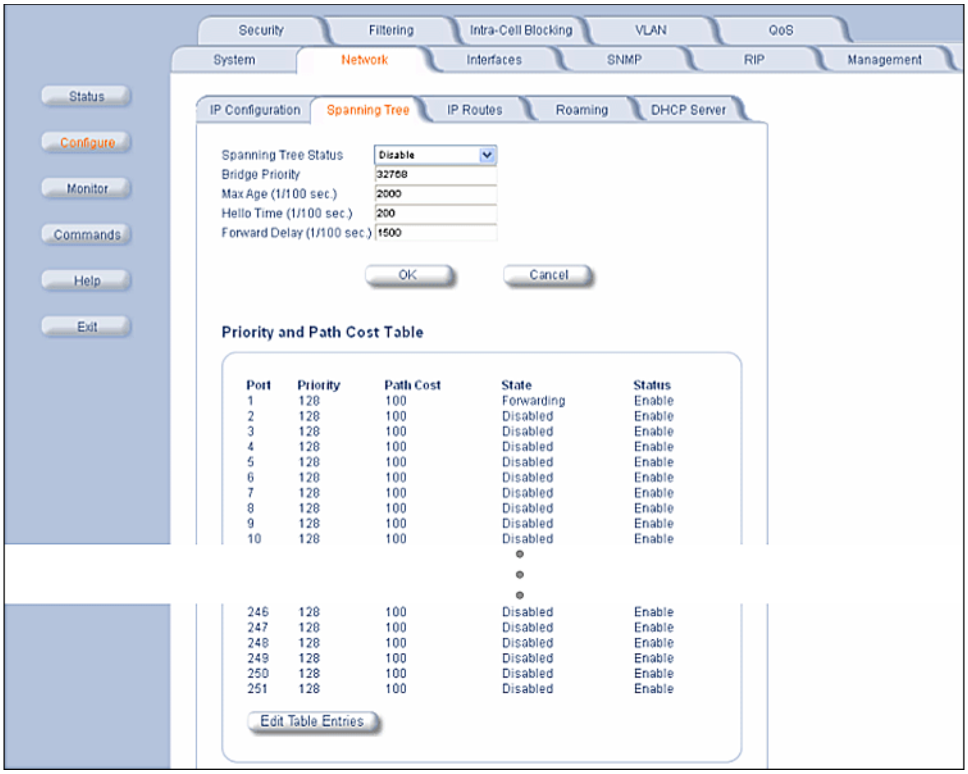
Configure Spanning Tree Options

This protocol is executed between the bridges to detect and logically remove redundant paths from the network. Spanning Tree can be used to prevent link-layer loops (broadcast is forwarded to all port where another device may forward it and, finally, it gets back to this unit; therefore, it is looping). Spanning Tree can also be used to create redundant links and operates by disabling links: hot standby customer is creating a redundant link without routing function.

If your network does not support Spanning Tree, be careful to avoid creating network loops between radios. For example, creating a WDS link between two units connected to the same Ethernet network creates a network loop (if spanning tree is disabled).

The Spanning Tree configuration options are advanced settings. Proxim recommends that you leave these parameters at their default values unless you are familiar with the Spanning Tree protocol.

Click the **Spanning Tree** tab to change Spanning Tree values.

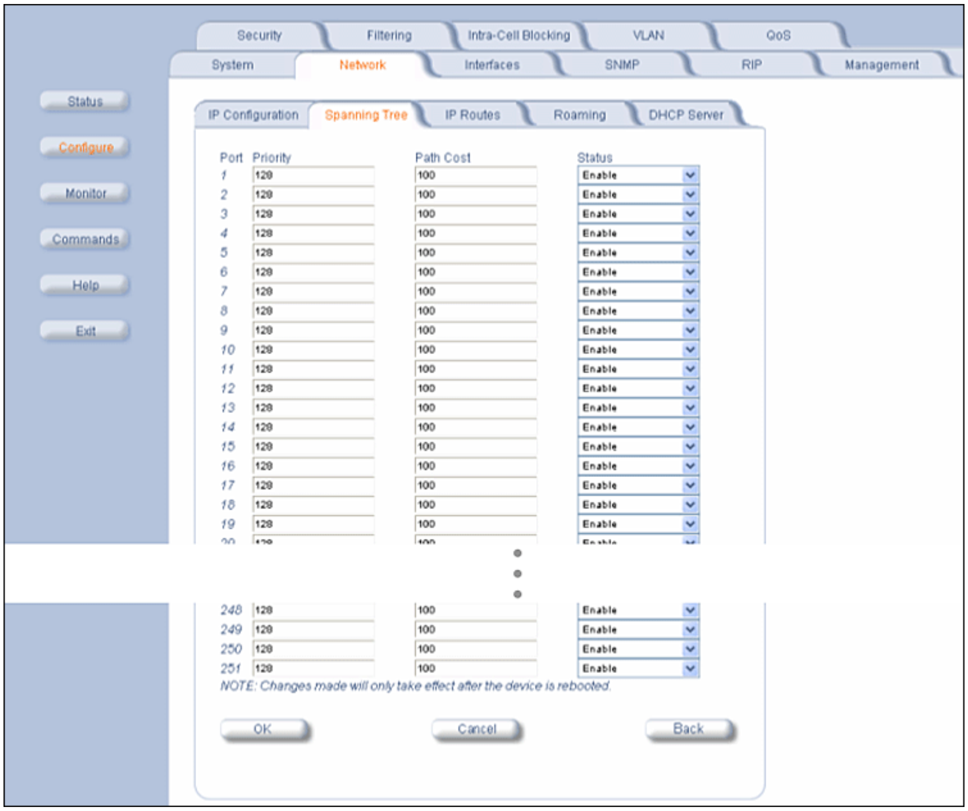


Spanning Tree Status	Disable
Bridge Priority	32768
Max Age (1/100 sec.)	2000
Hello Time (1/100 sec.)	200
Forward Delay (1/100 sec.)	1500

Priority and Path Cost Table

Port	Priority	Path Cost	State	Status
1	128	100	Forwarding	Enable
2	128	100	Disabled	Enable
3	128	100	Disabled	Enable
4	128	100	Disabled	Enable
5	128	100	Disabled	Enable
6	128	100	Disabled	Enable
7	128	100	Disabled	Enable
8	128	100	Disabled	Enable
9	128	100	Disabled	Enable
10	128	100	Disabled	Enable
246	128	100	Disabled	Enable
247	128	100	Disabled	Enable
248	128	100	Disabled	Enable
249	128	100	Disabled	Enable
250	128	100	Disabled	Enable
251	128	100	Disabled	Enable

Click **Edit Table Entries** to make changes; enter your changes and click **OK**.

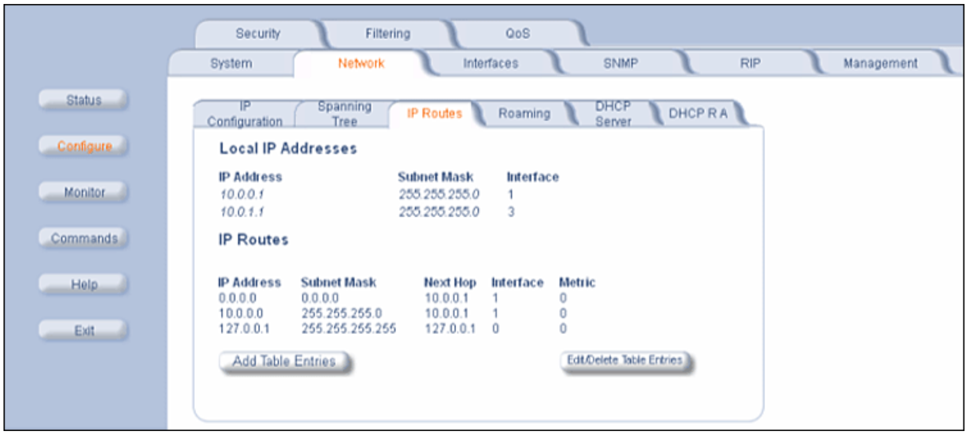


Port	Priority	Path Cost	Status
1	128	100	Enable
2	128	100	Enable
3	128	100	Enable
4	128	100	Enable
5	128	100	Enable
6	128	100	Enable
7	128	100	Enable
8	128	100	Enable
9	128	100	Enable
10	128	100	Enable
11	128	100	Enable
12	128	100	Enable
13	128	100	Enable
14	128	100	Enable
15	128	100	Enable
16	128	100	Enable
17	128	100	Enable
18	128	100	Enable
19	128	100	Enable
20	128	100	Enable
248	128	100	Enable
249	128	100	Enable
250	128	100	Enable
251	128	100	Enable

NOTE: Changes made will only take effect after the device is rebooted.

Configure IP Routes (Routing Mode only)

Click **Configure** > **Network** > **IP Routes** to configure IP routes. You cannot configure IP Routes in **Bridge** mode. In **Routing** mode, the **Add Table Entries** and **Edit/Delete Table Entries** buttons are enabled.



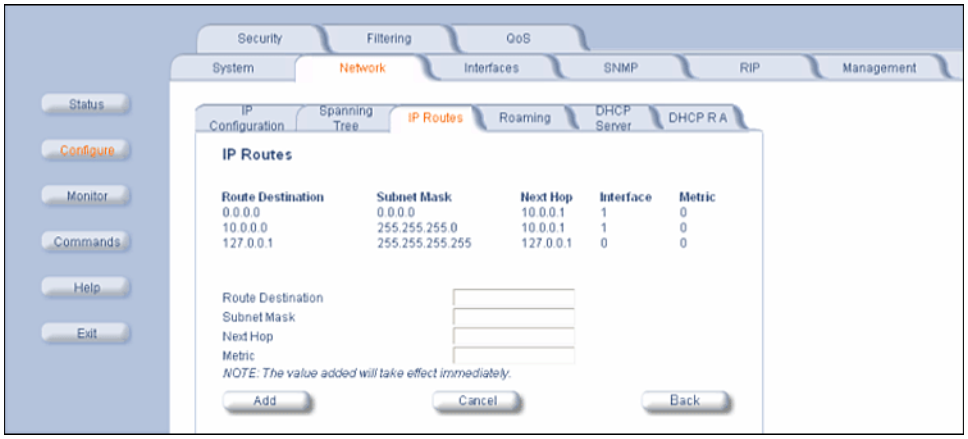
Local IP Addresses

IP Address	Subnet Mask	Interface
10.0.0.1	255.255.255.0	1
10.0.1.1	255.255.255.0	3

IP Routes

IP Address	Subnet Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	10.0.0.1	1	0
10.0.0.0	255.255.255.0	10.0.0.1	1	0
127.0.0.1	255.255.255.255	127.0.0.1	0	0

Click the **Add** button to add entries; a window such as the following is displayed:



IP Routes

Route Destination	Subnet Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	10.0.0.1	1	0
10.0.0.0	255.255.255.0	10.0.0.1	1	0
127.0.0.1	255.255.255.255	127.0.0.1	0	0

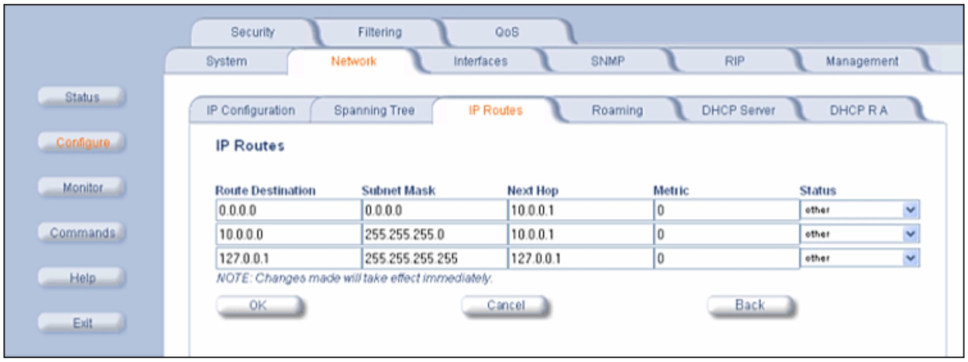
Route Destination
Subnet Mask
Next Hop
Metric

NOTE: The value added will take effect immediately.

Enter the route information and click **Add**. The **IP Address** and **Subnet Mask** combination is validated for a proper combination.

NOTE: *When adding a new entry, the IP address of the Route Destination must be in either the Ethernet subnet or in the wireless subnet of the unit.*

Click the **Edit/Delete Table Entries** button to make changes to or delete existing entries.



IP Routes

Route Destination	Subnet Mask	Next Hop	Metric	Status
0.0.0.0	0.0.0.0	10.0.0.1	0	other
10.0.0.0	255.255.255.0	10.0.0.1	0	other
127.0.0.1	255.255.255.255	127.0.0.1	0	other

NOTE: Changes made will take effect immediately.

Edit the route information and click **OK**. The IP address and subnet mask combination is validated for a proper combination.

Enable or Disable Roaming

Roaming Overview

Roaming is a feature by which an SU terminates the session with the current BSU and starts the registration procedure with another BSU when it finds the quality of the other BSU to be better. Roaming provides MAC level connectivity to the SU that roams from one BSU to another. Roaming takes place across the range of frequencies and channel bandwidths (5, 10, or 20 MHz) that are available per configuration. The current release offers handoff times of up to a maximum of 80 ms. This is fast enough to allow the SU to seamlessly roam from one BSU to the other therefore supporting session persistence for delay-sensitive applications. The feature also functions as BSU backup in case the current BSU fails or becomes unavailable.

The Roaming feature lets the SU monitor local SNR and data rate for all frames received from the current BSU. As long as the average local SNR for the current BSU is greater than the slow scanning threshold, and the number of retransmitted frames is greater than the slow scanning threshold given in percentage, the SU does not scan other channels for a better BSU.

- The ***normal scanning*** procedure starts when the average local SNR for the current BSU is less than or equal to the slow scanning threshold and the number of retransmitted frames is greater than the slow scanning threshold given in percentage. During the normal scanning procedure the SU scans the whole list of active channels while maintaining the current session uninterrupted.
- ***Fast scanning*** is the scanning procedure performed when the average local SNR for the current BSU is very low (below the fast scanning threshold) and the number of retransmitted frames is greater than the fast scanning retransmission threshold given in %, so that the current session should terminate as soon as possible. During this procedure, the SU scans other active channels as fast as possible.

Roaming can only occur if the normal scanning or fast scanning procedure is started under the following conditions:

1. If the roaming is started from the normal scanning procedure (after the SU scans all the active channels), the SU selects the BSU with the best SNR value on all available channels. The SU roams to the best BSU only if the SNR value for the current BSU is still below the slow scanning SNR threshold, and best BSU offers a better SNR value for at least roaming threshold than the current BSU. The SU starts a new registration procedure with the best BSU without ending the current session.
2. If the roaming is started from the fast scanning procedure, the SU selects the first BSU that offers better SNR than the current BSU, and starts a new registration procedure with the better BSU without ending the current session.

Roaming with Dynamic Data Rate Selection (DDRS) Enabled

When an SU roams from BSU-1 to BSU-2 and DDRS is enabled, the data rate at which the SU connects to BSU-2 is the default DDRS data rate. If this remains at the factory default of 6 Mbps, there can be issues with the application if it requires more then 6 Mbps (for example multiple video streams).

Applications requiring a higher data rate could experience a slight data loss during the roaming process while DDRS selects a higher rate (based upon link conditions).

When the applications re-transmit at a possibly slower rate, the WORP protocol initially services the data at 6 Mbps and increases the data rate up to the "Maximum DDRS Data Rate" (*ddrsmaxdatarate*) one step at a time. Because the applications are not being serviced at the best possible rate, they further slow down the rate of data send.

The DDRS algorithm requires data traffic (a minimum of 128 frames) to raise the rate to a higher value. Although roaming occurs successfully, the previous scenario causes applications to drop their sessions; hence session persistence is not maintained.

For a discussion on how to configure DDRS, see Dynamic Data Rate Selection (DDRS).

NOTE: *You must know the data rate required for the applications running and you must ensure (during network deployment) that the ranges and RF links can support the necessary data rate. You also must set the default DDRS data rate at the capacity necessary for the application so that it connects to the next Base Station at the required capacity if roaming occurs. Set the "Default DDRS Data Rate" (ddrsdefdatarate) to a greater value (24, 36, 48 or 54 Mbps, for example) for applications requiring session persistence when roaming occurs.*

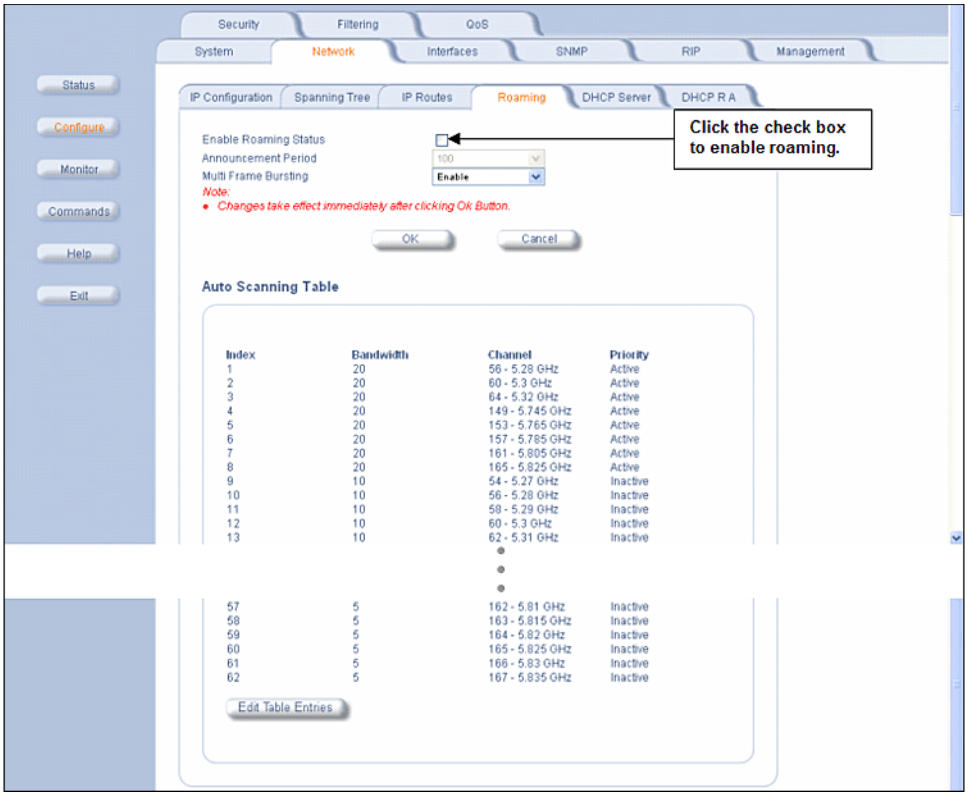
Configuring Roaming

Click **Configure** > **Network** > **Roaming** to configure Roaming. The screen differs depending on whether the unit is configured as a BSU or as an SU.

BSU Screen

Enable or disable the Roaming feature by selecting the **Enable Roaming Status** check box. The default value is disabled (clear). If you enable roaming, you may set the **Announcement Period** (from 25 to 100 ms, default is 100 ms).

On this screen you may also enable or disable the **Multi-Frame Bursting** (default value is enabled).



Click the check box to enable roaming.

Enable Roaming Status □
Announcement Period 100
Multi Frame Bursting Enable

Note:
- *Changes take effect immediately after clicking Ok Button.*

Auto Scanning Table

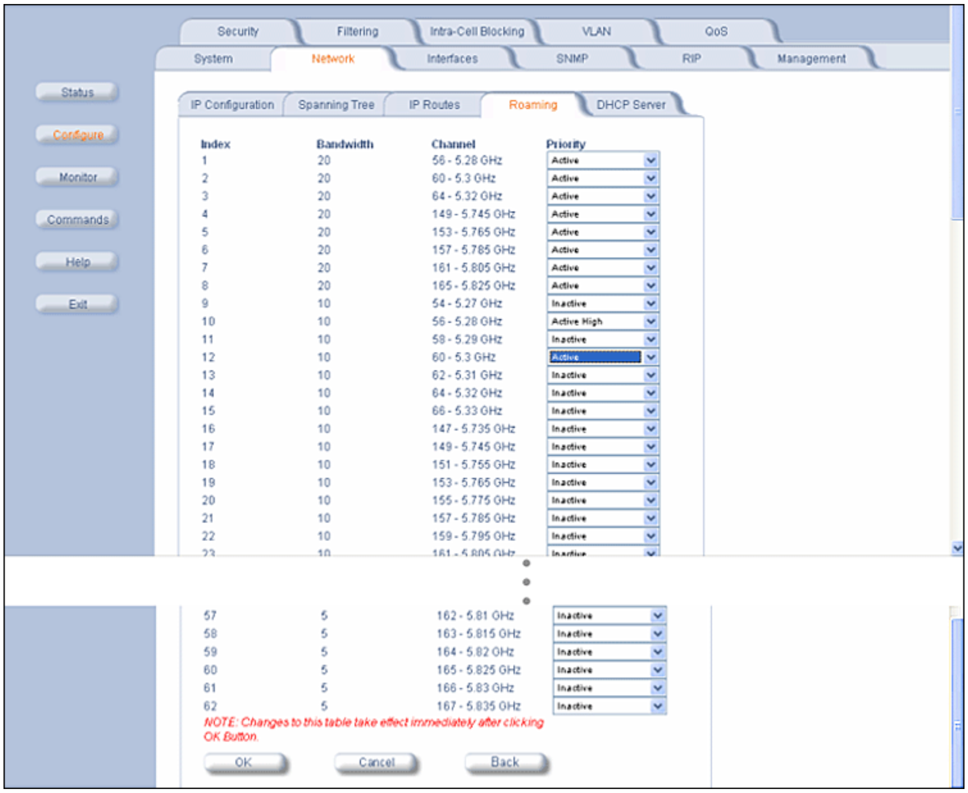
Index	Bandwidth	Channel	Priority
1	20	56 - 5.28 GHz	Active
2	20	60 - 5.3 GHz	Active
3	20	64 - 5.32 GHz	Active
4	20	149 - 5.745 GHz	Active
5	20	153 - 5.765 GHz	Active
6	20	157 - 5.785 GHz	Active
7	20	161 - 5.805 GHz	Active
8	20	165 - 5.825 GHz	Active
9	10	54 - 5.27 GHz	Inactive
10	10	56 - 5.28 GHz	Inactive
11	10	58 - 5.29 GHz	Inactive
12	10	60 - 5.3 GHz	Inactive
13	10	62 - 5.31 GHz	Inactive
		● ● ●	
57	5	162 - 5.81 GHz	Inactive
58	5	163 - 5.815 GHz	Inactive
59	5	164 - 5.82 GHz	Inactive
60	5	165 - 5.825 GHz	Inactive
61	5	166 - 5.83 GHz	Inactive
62	5	167 - 5.835 GHz	Inactive

An SU scans all available channels for a given bandwidth during roaming. In order to reduce the number of channels an SU has to scan and thus decrease the roaming time, a channel priority list that tells the SU what channels to scan is implemented. Each channel in the channel priority list is specified with its corresponding bandwidth and the priority with which it should be scanned, either "Active" (standard priority), "Active High" (high priority), or "Inactive".

An SU will scan all channels indicated as "Active" during roaming. However, it will scan active channels indicated as "High Priority" before scanning active channels indicated as standard priority. Channels that are not going to be used in the wireless network should be configured as "Inactive" so that the SU can skip over those channels during scanning saving this way time.

A BSU broadcasts the channel priority list to all valid authenticated SUs in its sector. It re-broadcasts the channel priority list to all SUs every time the list is updated on the BSU.

Click **Edit Table Entries** to make changes; enter your changes and click **OK**.



Index	Bandwidth	Channel	Priority
1	20	56 - 5.28 GHz	Active
2	20	60 - 5.3 GHz	Active
3	20	64 - 5.32 GHz	Active
4	20	149 - 5.745 GHz	Active
5	20	153 - 5.765 GHz	Active
6	20	157 - 5.785 GHz	Active
7	20	161 - 5.805 GHz	Active
8	20	165 - 5.825 GHz	Active
9	10	54 - 5.27 GHz	Inactive
10	10	56 - 5.28 GHz	Active High
11	10	58 - 5.29 GHz	Inactive
12	10	60 - 5.3 GHz	Active
13	10	62 - 5.31 GHz	Inactive
14	10	64 - 5.32 GHz	Inactive
15	10	66 - 5.33 GHz	Inactive
16	10	147 - 5.735 GHz	Inactive
17	10	149 - 5.745 GHz	Inactive
18	10	151 - 5.755 GHz	Inactive
19	10	153 - 5.765 GHz	Inactive
20	10	155 - 5.775 GHz	Inactive
21	10	157 - 5.785 GHz	Inactive
22	10	159 - 5.795 GHz	Inactive
23	10	161 - 5.805 GHz	Inactive
57	5	162 - 5.81 GHz	Inactive
58	5	163 - 5.815 GHz	Inactive
59	5	164 - 5.82 GHz	Inactive
60	5	165 - 5.825 GHz	Inactive
61	5	166 - 5.83 GHz	Inactive
62	5	167 - 5.835 GHz	Inactive

NOTE: Changes to this table take effect immediately after clicking OK Button.

Note that an SU may roam from one BSU with a bandwidth setting to another BSU with a different bandwidth setting. Since in this case more channels need to be scanned than with only one channel bandwidth setting, it is important that the channel priority list mentioned above is properly used to limit scanning time.

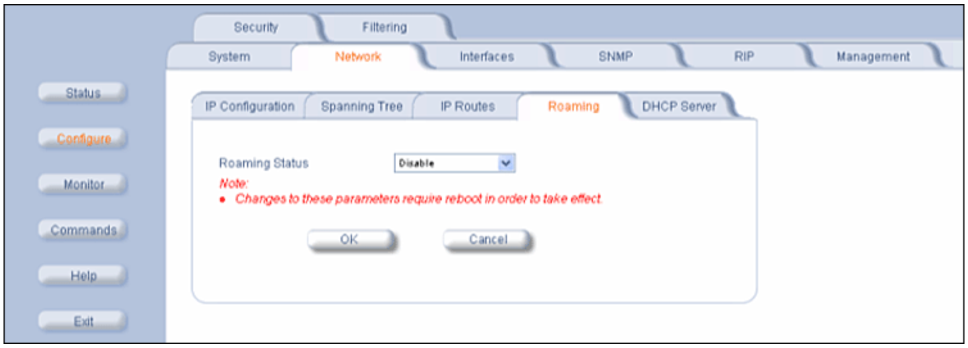
When **Scanning Across Bandwidth** on the SU is enabled (see Interface Parameters), the SU supports bandwidth selection of the communications channel of either 20 MHz, 10 MHz, or 5 MHz. This allows the BSUs in the network to be set to different bandwidths while an SU can still roam from one BSU to the next, because it will not only scan other frequencies (when the signal level or quality are lower than the threshold) but it will also switch to other bandwidths to find a BSU that may be on another bandwidth than its current one.

During roaming, the SU will start scanning first the channels on its *current* bandwidth from the “Active” channel list provided by the BSU in order to find a BSU to register, since that is the most likely setting for other BSUs in the network. If the SU cannot find an acceptable roaming candidate, it will switch bandwidth and start scanning channels on that corresponding bandwidth from the “Active” channel list provided by the BSU. The process is repeated until the SU finds an appropriate BSU to register.

In the example above, an SU whose current bandwidth is 20 MHz will start scanning all active channels within the bandwidth of 20 MHz. If it cannot find a suitable BSU, it will switch to a 10 MHz bandwidth and start scanning all active channels within that bandwidth, in this case channel 56 first since it is configured as high priority and channel 60 next. No channels will be scanned on the 5 MHz bandwidth since all those channels are configured as inactive.

SU Screen

Enable or disable the Roaming feature in the **Roaming Status** drop-down box. The default value is disabled.



Roaming Status: Disable

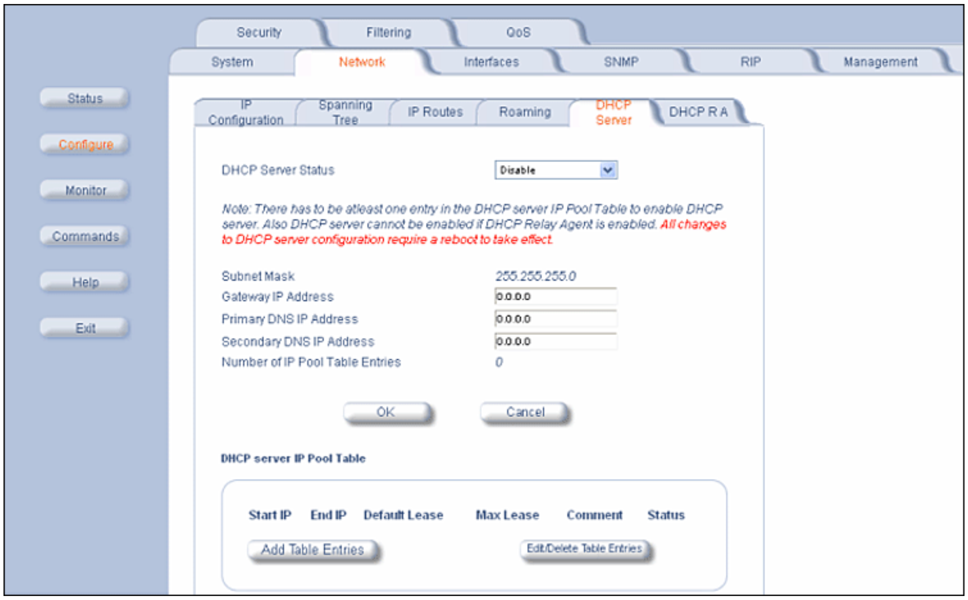
Note:

- Changes to these parameters require reboot in order to take effect

NOTE: *To enable roaming, you must enable* **Roaming Status** *on both the BSU and the SU.*

Enable and Configure the DHCP Server

Click **Configure** > **Network** > **DHCP Server** to enable the unit on a DHCP Server. The **Gateway IP Address** and **Primary DNS IP Address** must be entered, there must be at least one entry in the DHCP Server IP Pool Table, and the DHCP Relay Agent must be disabled, in order to enable the DHCP Server.



DHCP Server Status: Disable

Note: There has to be atleast one entry in the DHCP server IP Pool Table to enable DHCP server. Also DHCP server cannot be enabled if DHCP Relay Agent is enabled. All changes to DHCP server configuration require a reboot to take effect.

Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0
Primary DNS IP Address: 0.0.0.0
Secondary DNS IP Address: 0.0.0.0
Number of IP Pool Table Entries: 0

DHCP server IP Pool Table

Start IP	End IP	Default Lease	Max Lease	Comment	Status

When enabled, the DHCP server allows allocation of IP addresses to hosts on the Ethernet side of the SU or BSU. Specifically, the DHCP Server feature lets the SU or BSU respond to DHCP requests from Ethernet hosts with the following information:

- Host IP address
- Gateway IP address
- Subnet Mask
- DNS Primary Server IP address
- DNS Secondary Server IP

The following parameters are configurable:

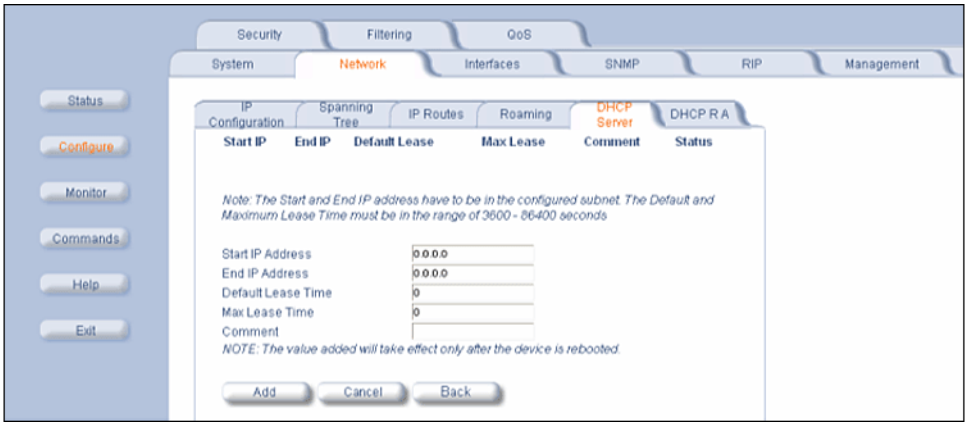
- **DHCP Server Status:** Verify that DHCP Relay Agent is disabled. After you have made at least one entry in the DHCP server IP Pool Table, enable DHCP Server by selecting “Enable” from the **DHCP Server Status** pull-down menu.

NOTE: *There must be at least one entry in the DHCP server IP Pool Table to enable DHCP server. Also, DHCP server cannot be enabled if DHCP Relay Agent is enabled.*

- **Subnet Mask:** The unit supplies this subnet mask in its DHCP response to a DHCP request from an Ethernet host. Indicates the IP subnet mask assigned to hosts on the Ethernet side using DHCP.
- **Gateway IP Address:** The unit supplies this gateway IP address in the DHCP response. Indicates the IP address of a router assigned as the default gateway for hosts on the Ethernet side.
- **Primary DNS IP Address:** The unit supplies this primary DNS IP address in the DHCP response. Indicates the IP address of the primary DNS server that hosts on the Ethernet side uses to resolve Internet host names to IP addresses
- **Secondary DNS IP Address:** The unit supplies this secondary DNS IP address in the DHCP response.
- **Number of IP Pool Table Entries:** The number of IP pool table entries is a read-only field that indicates the total number of entries in the DHCP server IP Pool Table. See Add Entries to the DHCP Server IP Pool Table.

Add Entries to the DHCP Server IP Pool Table

You can add up to 20 entries in the IP Pool Table. An IP address can be added if the entry's network ID is the same as the network ID of the device. To add an entry click **Add Table Entries**.



Start IP	End IP	Default Lease	Max Lease	Comment	Status

Note: The Start and End IP address have to be in the configured subnet. The Default and Maximum Lease Time must be in the range of 3600 - 86400 seconds

Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Default Lease Time	0
Max Lease Time	0
Comment	

NOTE: The value added will take effect only after the device is rebooted.

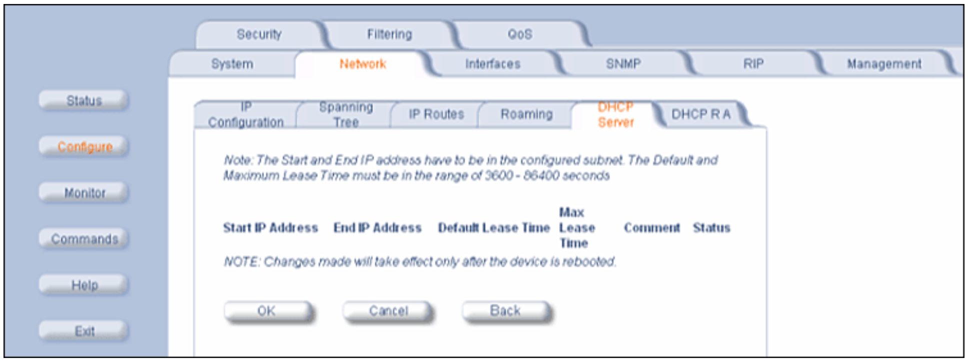
Enter the following parameters and click **Add**:

NOTE: *After adding entries, you must reboot the unit before the values take effect.*

- **Start IP Address:** Indicates the starting IP address that is used for assigning address to hosts on the Ethernet side in the configured subnet.
- **End IP Address:** Indicates the ending IP address that is used for assigning address to hosts on the Ethernet side in the configured subnet.
- **Default Lease Time:** Specifies the default lease time for IP addresses in the address pool. The value is 3600-86400 seconds.
- **Max Lease Time:** The maximum lease time for IP addresses in the address pool. The value is 3600-86400 seconds.
- **Comment:** The comment field is a descriptive field of up to 255 characters.

Edit/Delete Entries to the DHCP Server IP Pool Table Entries

Click **Edit/Delete Table Entries** to make changes; enter your changes and click **OK**.



Note: The Start and End IP address have to be in the configured subnet. The Default and Maximum Lease Time must be in the range of 3600 - 86400 seconds

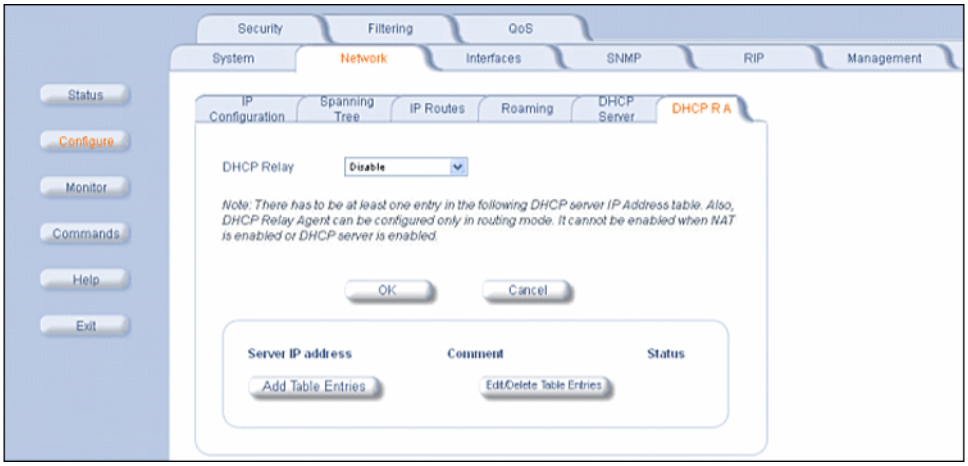
Start IP Address	End IP Address	Default Lease Time	Max Lease Time	Comment	Status

NOTE: Changes made will take effect only after the device is rebooted.

Enable the DHCP Relay Agent (Routing Mode Only)

Click **Configure** > **Network** > **DHCP RA** to enable the unit's DHCP Relay Agent. When enabled, the DHCP relay agent forwards DHCP requests to the set DHCP server. There must be at least one entry in the corresponding Server IP Address table in order to enable the DHCP Relay Agent.

Note that DHCP Relay Agent parameters are configurable only in **Routing** mode. It cannot be enabled when NAT or DHCP Server is enabled.



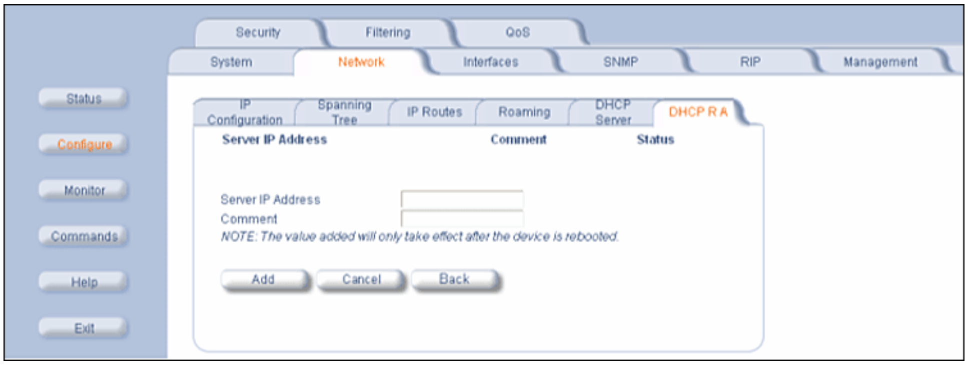
DHCP Relay: Disable

Note: There has to be at least one entry in the following DHCP server IP Address table. Also, DHCP Relay Agent can be configured only in routing mode. It cannot be enabled when NAT is enabled or DHCP server is enabled.

Server IP address	Comment	Status

Add Entries to the DHCP Relay Agent Table

To add entries to the table of DHCP Relay Agents, click **Add Table Entries**; the following window is displayed:



Server IP Address	Comment	Status

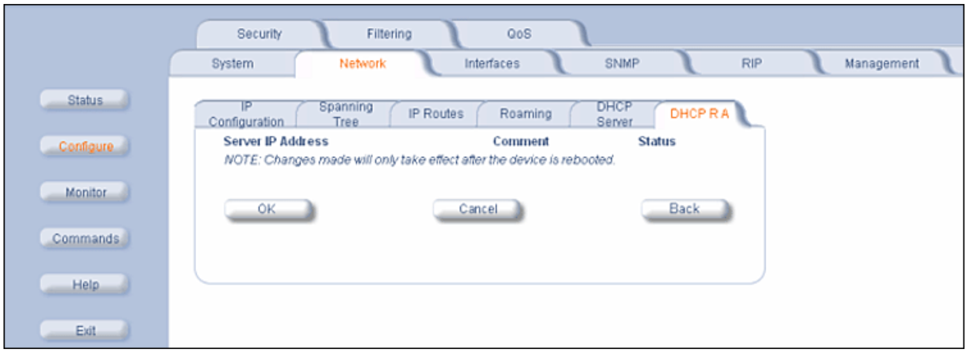
Server IP Address
Comment

NOTE: The value added will only take effect after the device is rebooted.

Enter the **Server IP Address** and any optional comments; click **Add**.

Edit/Delete Entries to the DHCP Relay Agent Table

Click **Edit/Delete Table Entries** to make changes; enter your changes and click **OK**.



Server IP Address **Comment** **Status**

NOTE: Changes made will only take effect after the device is rebooted.

Interface Parameters

Configure the Wireless Interface

To configure the wireless interface, click **Configure** > **Interfaces** > **Wireless**.

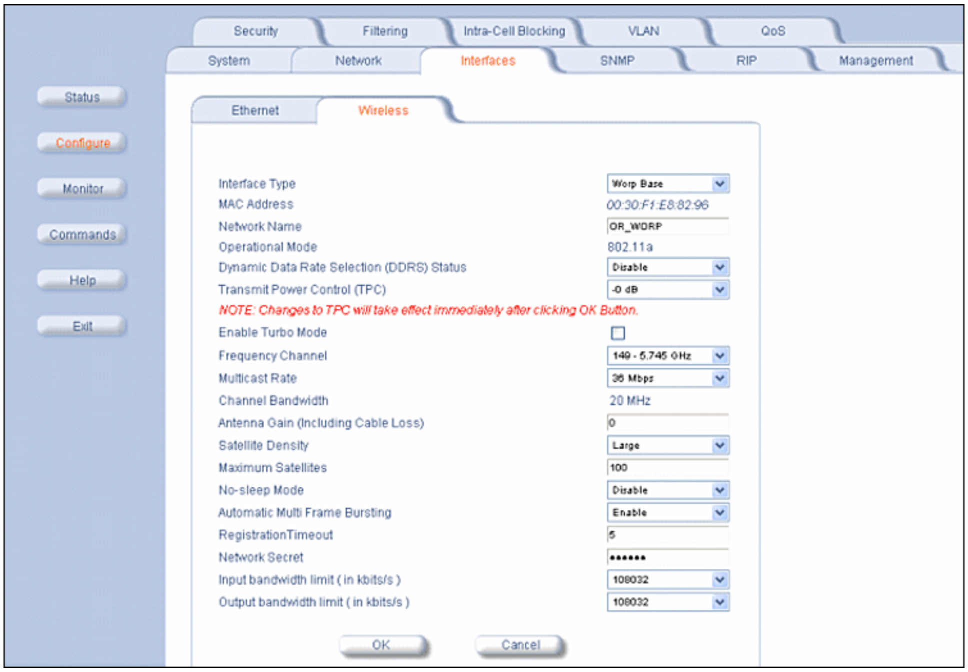
For Base Station units, the wireless interface can be placed in either WORP Base or WORP Satellite mode (selected from the **Interface Type** drop-down box). SUs can be placed only in WORP Satellite mode. The wireless interface settings depend upon whether the mode is Base or Satellite.

The Wireless Outdoor Router Protocol (WORP) is a polling algorithm designed for wireless outdoor networks. WORP takes care of the performance degradation incurred by the so-called “hidden-node” problem, which can occur when wireless LAN technology is used for outdoor building-to-building connectivity. In this situation, when multiple radios send an RTS, if another radio is transmitting, it corrupts all data being sent, degrading overall performance. The WORP polling algorithm ensures that these collisions cannot occur, which increases the performance of the overall network significantly.

WORP dynamically adapts to the number of SUs that are active on the network and the amount of data they have queued to send.

The following are examples of the Wireless window when the country selected is US, and for countries different than the US:

Base Mode – US Country



Interface Type	Worp Base
MAC Address	00:30:F1:E8:82:96
Network Name	OR_WORP
Operational Mode	802.11a
Dynamic Data Rate Selection (DDRS) Status	Disable
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

Enable Turbo Mode	□
Frequency Channel	149 - 5.745 GHz
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Antenna Gain (Including Cable Loss)	0
Satellite Density	Large
Maximum Satellites	100
No-sleep Mode	Disable
Automatic Multi Frame Bursting	Enable
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032

The following parameters may be configured or viewed:

- **Interface Type:** The interface type can be **WORP Satellite** or **WORP Base**.
- **MAC Address:** The factory-assigned MAC address of the unit. This is a read-only field.
- **Network Name:** A Network Name is a name given to a network so that multiple networks can reuse the same frequency without problems. An SU can only register to its base if it has the same Network Name. The Network Name is one of the parameters that allow a Subscriber Unit to register on a Base Station. The **Base Station System Name** and **Frequency Channel** also are parameters to guide the SU to the proper BSU on the network, but they provide no

security. Basic security is provided through encryption, as it causes none of the messages to be sent in the clear. Further security is provided by mutual authentication of the BSU and SU using the **Network Secret**. The Network Name can be 2 to 32 characters in length.

- **Operational Mode:** This field indicates the operational mode of the unit – 11a, 11b, or 11g – depending upon the specific Tsunami MP.11. This operational mode cannot be changed as it is based upon a license file.
- **Dynamic Data Rate Selection (DDRS) Status:** The **DDRS Status** is configurable only for the **WORP Base Mode**. For **WORP Base Mode**, select the **DDRS Status** “Enable” or “Disable” from the drop-down box provided.

  For the **WORP Satellite Mode**, **DDRS Status** is read-only parameter and its value is based upon the **WORP Base** to which this SU is associated.

  When you enable or disable DDRS on the BSU, the BSU sends an announcement to the SUs and the SUs enable or disable DDRS automatically.
- **Transmit Power Control (TPC):** By default, the unit lets you transmit at the maximum output power for the country or regulatory domain and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country. Also, most countries in the ETSI regulatory domain require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits. You can see your unit’s current output power for the selected frequency in the event log.

  The event log shows the selected power for all data rates, so you must look up the proper data rate to determine the actual power level.

  NOTE: *This feature only lets you decrease your output power; it does not let you increase your output power beyond the maximum allowed defaults for your frequency and country.*

  Select one of the following options and click **OK** at the bottom of the window. Your original output power is adjusted relative to the value selected. The new setting takes effect immediately without rebooting:

TPC Selection (dB)	Maximum TX Power (dBm)
0 (default)	16
-3	13
-6	10
-9	7
-12	4
-15	1
-18 (minimum TPC level)	0

NOTE: *24 Mbps and lower modulation have maximum +16 dBm TX power, 36 Mbps has maximum +13 dBm TX power, 48 Mbps has maximum +12 dBm TX power, and 54 Mbps has maximum +11 dBm TX power. Because higher modulation has a lower maximum TX power, the total TPC range is smaller at a higher data rate. Because the minimum TX power is equal for all data rates, each TPC selection has constant TX power for all data rates except where the maximum TX power is limited.*

- **Enable Turbo Mode:** Check this box to enable Turbo Mode. Turbo Mode is supported only in the United States, and only for the 5054-R.

  Enabling turbo mode, in its current implementation, allows the unit to use two adjacent frequency channels to transmit and receive a signal. By enabling turbo mode, the receive sensitivity improves by 4 dB for the 36 Mbps data rate and by 2 dB for the 24 Mbps data rate.

  NOTE: *The additional sensitivity is provided with the impact of using twice as much spectrum and thus increasing the opportunity of interference and decreased ability for system collocation. Generally, Turbo mode is not recommended except when the extra sensitivity is absolutely required.*
- **Frequency Channel:** The frequency channel indicates the band center frequency the unit uses for communicating with peers. This frequency channel can be set in several ranges, depending upon regulatory domain. Refer to Country Codes and Channels for channelization information.

For countries in which DFS is not enabled, the **Frequency Channel** list displays only the channels and frequencies allowed for the selected country.

- **Multicast Rate:** The rate at which data is to be transferred. This drop down box is unavailable when DDRS is enabled.

  The default multicast rate for the unit is 36 Mbps. The SU must never be set to a lower data rate than the BSU because timeouts will occur at the BSU and communication will fail.

  Selections for multicast rate for 5, 10, and 20 MHz channel bandwidths are shown in the following table:

5 MHz	10 MHz	20 MHz
1.5	3	6
2.25	4.5	9
3	6	12
4.5	9	18
6	12	24
9	18	36
12	24	48
13.5	27	54

- **Antenna Gain (BSU only):** You can modify the sensitivity of the radio card when detecting radar signals in accordance with ETSI and FCC Dynamic Frequency Selection (DFS) requirements. Given the radar detection threshold is fixed by ETSI and the FCC and that a variety of antennas with different gains may be attached to the unit, you must adjust this threshold to account for higher than expected antenna gains and avoid false radar detection events. This can result in the units constantly changing frequency channels.

  You can configure the threshold for radar detection at the radio card to compensate for increased external antenna gains.

  The Antenna Gain value ranges from 0 to 35. The default value is 0.

- **Satellite Density:** The **Satellite Density** setting is a valuable feature for achieving maximum bandwidth in a wireless network. It influences the receive sensitivity of the radio interface and improves operation in environments with a high noise level. Reducing the sensitivity of the unit enables unwanted “noise” to be filtered out (it disappears under the threshold).

  You can configure the **Satellite Density** to be **Large**, **Medium**, **Small**, **Mini**, or **Micro**. The default value for this setting is Large. The smaller settings are appropriate for high noise environments; a setting of **Large** would be for a low noise environment.

  A long distance link may have difficulty maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10 dB below the present signal strength.

  If the Signal-to-Noise Ratio (SNR) is not sufficient, you may need to set a lower data rate or use antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint configuration, the BSU should have a density setting suitable for all of its registered SUs, especially the ones with the lowest signal levels (longest links).

  Take care when configuring a remote interface; check the available signal level first, using Remote Link Test.

  WARNING: When the remote interface accidentally is set at too small a value and communication is lost, it cannot be reconfigured remotely and a local action is required to bring the communication back. Therefore, the best place to experiment with the level is at the unit that can be managed without going through the link; if the link is lost, the setting can be adjusted to the correct level to bring the link back.

  To set the **Satellite Density**, click the **Configure** button, then the **Interfaces** tab and the **Wireless** sub-tab. Make your density selection from the drop-down menu. This setting requires a reboot of the unit.

Sensitivity threshold settings related to the density settings for the unit are:

Set Satellite Density to:	For a Receive Sensitivity Threshold of:	And a Defer Threshold of:
Large	-95 dBm	-62 dBm
Medium	-86 dBm	-62 dBm
Small	-78 dBm	-52 dBm
Mini	-70 dBm	-42 dBm
Micro	-62 dBm	-36 dBm

- **Maximum Satellites (BSU only):** You can specify a maximum value of 250 in this field, because up to 250 SUs can be connected to a BSU. If a BSU already has as many SUs as specified in this field, a new SU cannot connect to the BSU.
- **No-Sleep Mode (BSU only):** No-Sleep Mode was a feature used to control jitter in Tsunami MP.11 products running 2.2.6, and earlier, versions of software. The introduction of QoS and the new WORP resource scheduling mechanism have eliminated the need for No-Sleep Mode. Furthermore, QoS provides better control over jitter and latency-sensitive applications (see QoS (Quality of Service) Parameters for details on configuration). This field is inactive and makes no difference whether is enabled or disabled.
- **Automatic Multi-Frame Bursting (BSU only):** In order to achieve higher throughput, WORP protocol allows each side (BSU or SU) to send a burst of up to 4 data messages instead of a single data message. The sole criteria for sending a burst is enough traffic to be sent out. This feature is called Multi-Frame Bursting support.

  Automatic Multi-Frame bursting optimizes multi-burst performance when configuring QoS high-priority Service Flows. Three scenarios may be defined:

  – *No Multi-Frame Burst Support* –To disable Multi-Frame burst support, click **Configure** > **Network** > **Roaming,** and select “Disable” on the drop-down box (see BSU Screen). In this case, each active SFC is limited to send a single data message. Total throughput available to remaining best effort traffic is around 76% of the maximum available throughput.

  Multi-Frame Burst Support – The system will enable Multi-Frame burst for *all* SFCs, but the maximum number of data messages sent in a burst will be defined by the parameter “Number of data messages in a burst” for each of the SFCs (see Service Flow Class (SFC). This scenario is set by clicking **Configure** > **Network** > **Roaming** and enabling Multi-Frame burst on the drop-down box (see BSU Screen), and disabling **Automatic Multi-Frame Bursting** (this parameter).

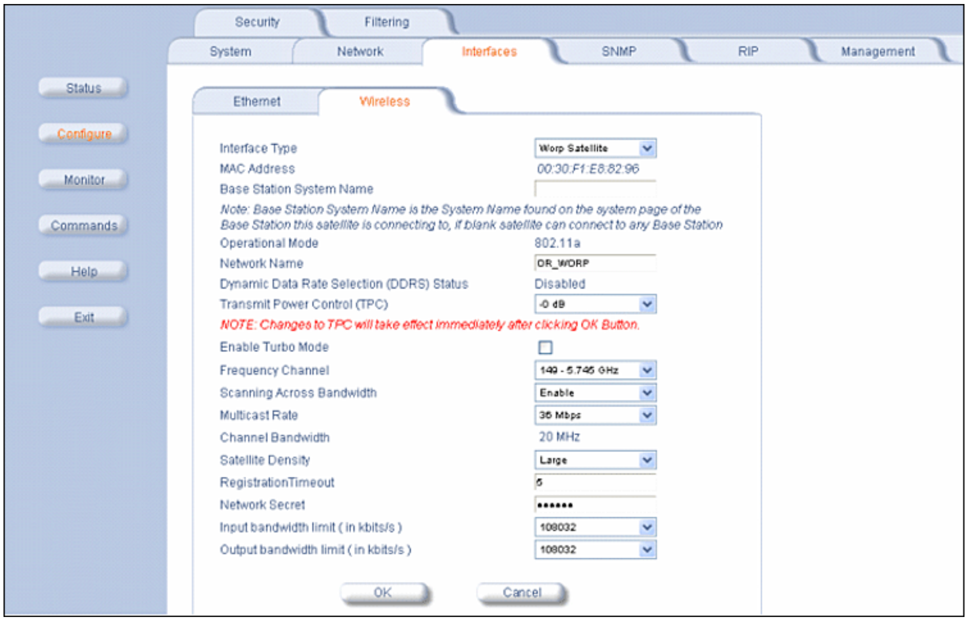
  The maximum number of data messages in a burst directly influences the total throughput of the system. Typical values are:

No. of messages in a burst:	% of the maximum throughput:
4	100%
3	97.6%
2	92.9%
1	76.2%

  – *Automatic Multi-Frame Burst Support* – The system will continuously be monitoring which of the active SFCs has the highest priority and dynamically enable Multi-Frame burst for the highest priority SFC only, keeping all the lower priority SFCs with Multi-Frame burst disabled. If there are multiple SFCs having the same, highest priority, all of them will have Multi-Frame burst enabled. The maximum number of data messages sent in a burst is defined by the parameter “Number of data messages in a burst” and it can be different for each SFC (see Service Flow Class (SFC)). This scenario is set by clicking **Configure** > **Network** > **Roaming** and enabling Multi-Frame burst on the drop-down box (see BSU Screen), and enabling **Automatic Multi-Frame Bursting** (this parameter). In this case, even the lowest priority SFC will have Multi-Frame burst dynamically enabled as long as it is the only SFC in the system that has traffic. By default, configuring even a single high priority SFC with automatic multi-frame bursting enabled will decrease throughput of low priority best-effort traffic to approximately 76% of maximum available throughput, because low priority traffic will have Multi-Frame burst disabled to optimize bandwidth for the high priority traffic.

- **Registration Timeout:** This is the registration process time-out of an SU on a BSU. Default is 5 seconds.
- **Network Secret:** A network secret is a secret password given to all nodes of a network. An SU can only register to a BSU if it has the same Network Secret. The Network Secret is sent encrypted and can be used as a security option.
- **Input / Output Bandwidth Limit:** These parameters limit the data traffic received on the wireless interface and transmitted to the wireless interface, respectively. Selections are in steps of 64 Kbps from 64 Kbps to 108,064 Kbps.

Satellite Mode – US Country



Interface Type	Worp Satellite
MAC Address	00:30:F1:E8:82:96
Base Station System Name	

Note: Base Station System Name is the System Name found on the system page of the Base Station this satellite is connecting to, if blank satellite can connect to any Base Station

Operational Mode	802.11a
Network Name	OR_WORP
Dynamic Data Rate Selection (DDRS) Status	Disabled
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

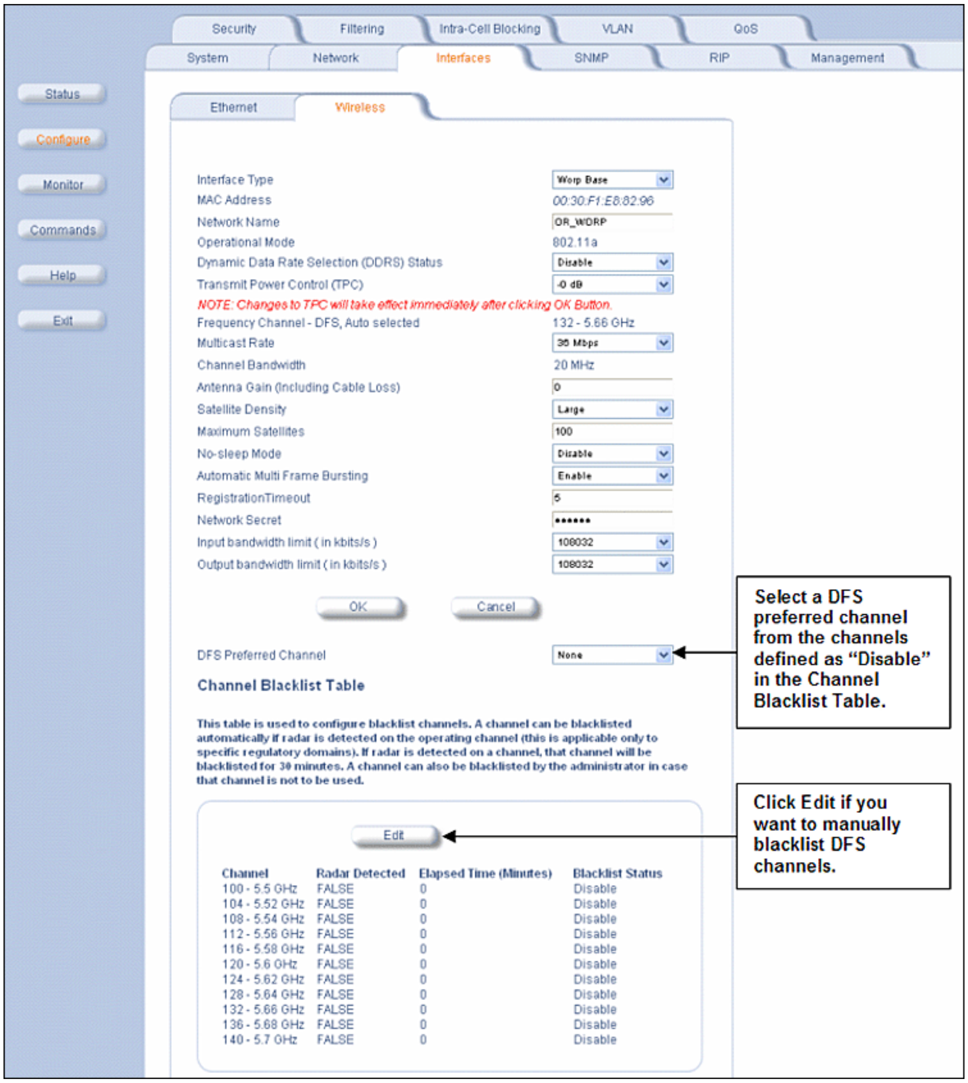
Enable Turbo Mode	□
Frequency Channel	149 - 5.745 GHz
Scanning Across Bandwidth	Enable
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Satellite Density	Large
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032

All the fields that are common to both the BSU and the SU are applicable here. The SU features two additional fields:

- **Base Station System Name (SU only):** The name found on the system page of the BSU to which this SU is connecting. This parameter can be used as an added security measure, and when there are multiple BSUs in the network and you want an SU to register with only one when it may actually have adequate signal strength for either. The System Name field is limited to a length of 32 bytes.

  If the Base Station System Name is left blank on the SU, it can register with any BSU with a matching Network Name and Network Secret.
- **Scanning Across Bandwidth (SU only):** Enable this field if you want the SU to scan across the whole range of channel bandwidths (5, 10, or 20 MHz) with or without roaming enabled. Disable this field if you wish the SU to scan only across its configured channel bandwidth.

Base Mode – Non-US Country



Interface Type	Worp Base
MAC Address	00:30:F1:E8:82:96
Network Name	OR_WORP
Operational Mode	802.11a
Dynamic Data Rate Selection (DDRS) Status	Disable
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

Frequency Channel - DFS, Auto selected	132 - 5.66 GHz
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Antenna Gain (Including Cable Loss)	0
Satellite Density	Large
Maximum Satellites	100
No-sleep Mode	Disable
Automatic Multi Frame Bursting	Enable
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032
DFS Preferred Channel	None

Select a DFS preferred channel from the channels defined as “Disable” in the Channel Blacklist Table.

Channel Blacklist Table

This table is used to configure blacklist channels. A channel can be blacklisted automatically if radar is detected on the operating channel (this is applicable only to specific regulatory domains). If radar is detected on a channel, that channel will be blacklisted for 30 minutes. A channel can also be blacklisted by the administrator in case that channel is not to be used.

Click Edit if you want to manually blacklist DFS channels.

Channel	Radar Detected	Elapsed Time (Minutes)	Blacklist Status
100 - 5.5 GHz	FALSE	0	Disable
104 - 5.52 GHz	FALSE	0	Disable
108 - 5.54 GHz	FALSE	0	Disable
112 - 5.56 GHz	FALSE	0	Disable
116 - 5.58 GHz	FALSE	0	Disable
120 - 5.6 GHz	FALSE	0	Disable
124 - 5.62 GHz	FALSE	0	Disable
128 - 5.64 GHz	FALSE	0	Disable
132 - 5.66 GHz	FALSE	0	Disable
136 - 5.68 GHz	FALSE	0	Disable
140 - 5.7 GHz	FALSE	0	Disable

The differences between the BSU Wireless interface screen for a non-US country and the equivalent screen for the US are:

- There is no **Turbo Mode**.
- **Frequency Channel** is not configurable. Instead the channel is auto-selected by the DFS process.

For descriptions of all the other fields that appear in both the US and non-US screen for the BSU, see Base Mode – US Country. In addition, the BSU screen for non-US countries contains these additional fields:

- **DFS Preferred Channel:** A single DFS preferred frequency channel on the BSU is provided so that when the DFS process starts the BSU will first try the DFS preferred channel before scanning all the other active channels in the DFS channel list. The DFS preferred channel must be selected from those channels indicated as “Disable” in the DFS channel blacklist list. It is not possible to select the DFS preferred channel from those channels in the DFS channel blacklist list indicated as “Enable”.
- **Channel Blacklist Table:** The DFS channel blacklist table shows all the channels in the current bandwidth and specifies the blacklist status of each channel as one of the following:
  - Enable – Channels that are made unavailable either for a certain period of time upon detection of a radar signal, or permanently because the operator has configured them as blacklisted. These channels are skipped over during DFS channel selection.

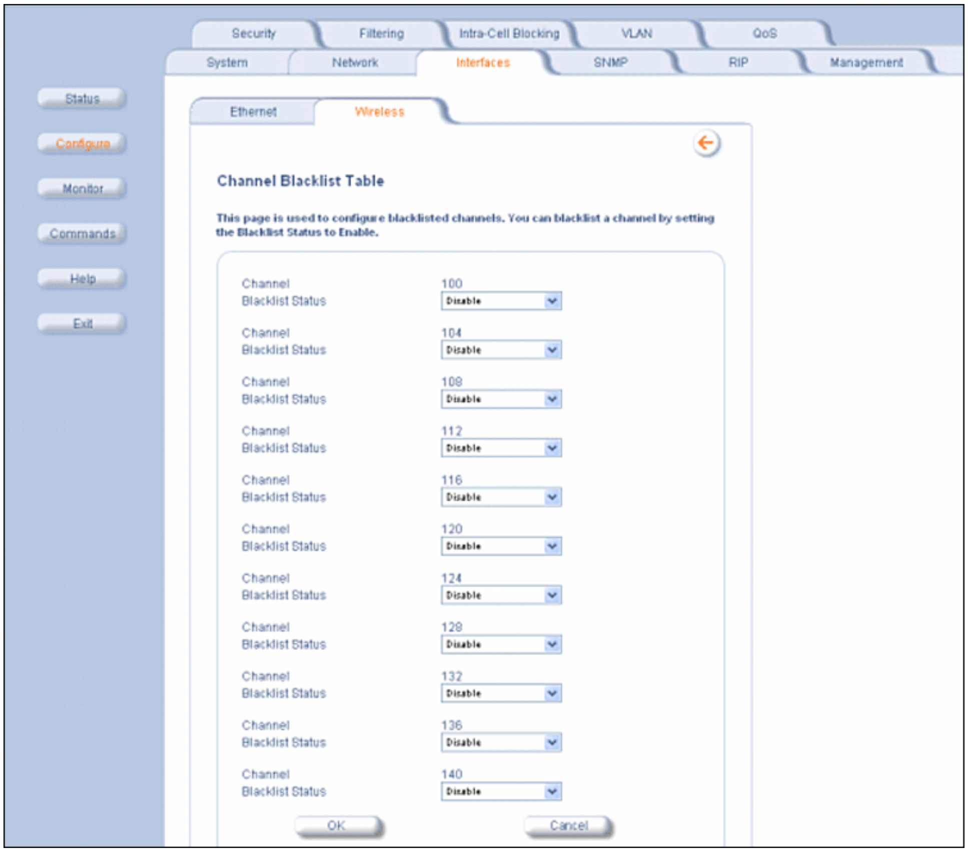
– Disable – Channels that are to be scanned during DFS.

Edit Entries to the Channel Blacklist Table

In accordance to the EN301-893 non-occupancy rule, when a radar signal is detected on any active channel, the blacklist status of that channel will change to “Enable” and the Radar Detected status will change to TRUE (see previous figure). The channel will not be used for a period of 30 minutes after the radar signal has been detected. The elapsed time is also shown in the DFS channel blacklist table. When the elapsed time for a channel in the blacklist is greater than or equal to 30 minutes, the blacklist status of the channel will change to Disable and the Radar Detected and Elapsed Time fields will change accordingly.

If an operator knows in advance on which channels a radar signal is likely to exist, those channels can be blacklisted and hence they will be skipped during DFS. Similarly, if the operator knows of channels where a radar signal is unlikely to be detected, those channels can be defined as active and hence they will be scanned during DFS. This makes the whole process more efficient.

When you click **Edit**, the channel blacklist table screen appears. Here you can manually configure each channel as “active” (Blacklist Status = Disable) or “blacklisted” (Blacklist Status = Enable). Enter your changes and click **OK**. To go back, click on the arrow button.

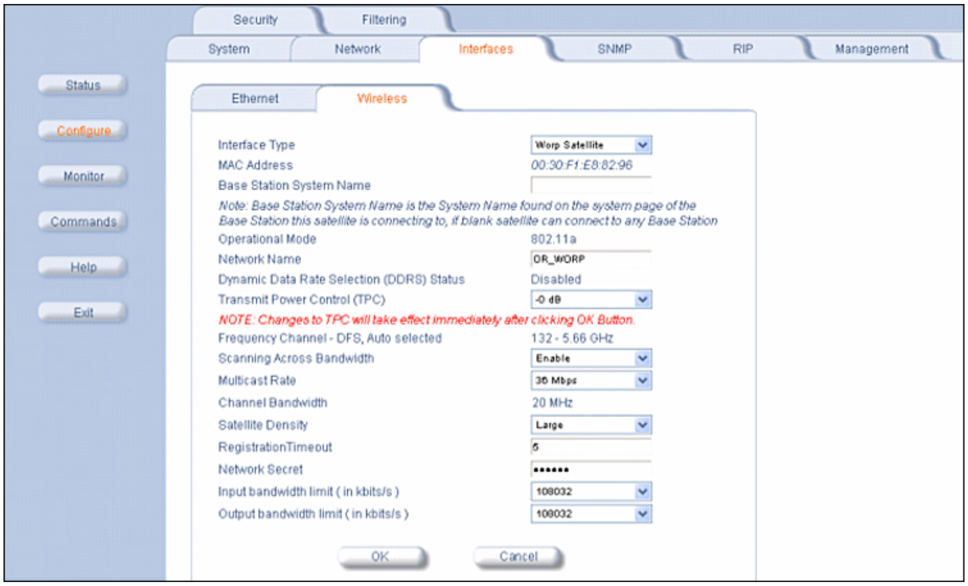


Channel Blacklist Table

This page is used to configure blacklisted channels. You can blacklist a channel by setting the Blacklist Status to Enable.

Channel	100
Blacklist Status	Disable
Channel	104
Blacklist Status	Disable
Channel	108
Blacklist Status	Disable
Channel	112
Blacklist Status	Disable
Channel	116
Blacklist Status	Disable
Channel	120
Blacklist Status	Disable
Channel	124
Blacklist Status	Disable
Channel	128
Blacklist Status	Disable
Channel	132
Blacklist Status	Disable
Channel	136
Blacklist Status	Disable
Channel	140
Blacklist Status	Disable

Satellite Mode – Non-US Country



Interface Type	Worp Satellite
MAC Address	*00:30:F1:E8:82:96*
Base Station System Name	

Note: Base Station System Name is the System Name found on the system page of the Base Station this satellite is connecting to, if blank satellite can connect to any Base Station

Operational Mode	802.11a
Network Name	OR_WORP
Dynamic Data Rate Selection (DDRS) Status	Disabled
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

Frequency Channel - DFS, Auto selected	132 - 5.66 GHz
Scanning Across Bandwidth	Enable
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Satellite Density	Large
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032

The differences between the SU Wireless interface screen for a non-US country and the equivalent screen for the US are:

- There is no **Turbo Mode**.
- **Frequency Channel** is not configurable. Instead the channel is auto-selected by the DFS process.

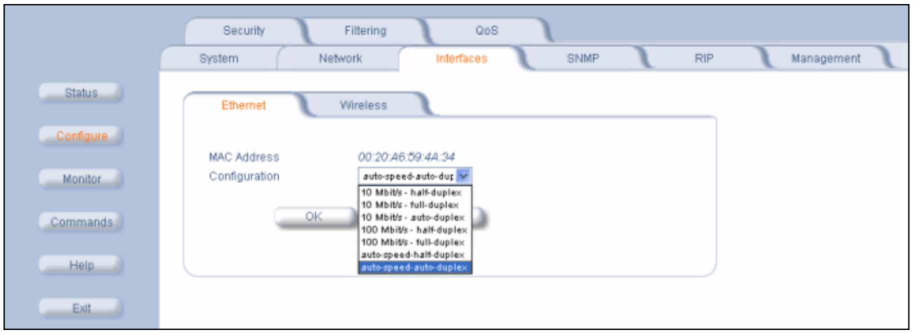
For descriptions of all other fields on this screen, see Satellite Mode – US Country.

Notes:

- Turbo mode is available only when the specified **Country** is US and only for the 5054.
- The list of parameters to configure for registration of the SU on a Base Station are:
  - Network Name
  - Base Station System Name (when used)
  - Channel Frequency
  - Encryption (when used)
  - Network Secret

Configure the Ethernet Interface

To set the Ethernet speed, duplex mode, and input and output bandwidth limits, click **Configure** > **Interfaces** > **Ethernet**.



MAC Address	*00:20:A6:59:4A:34*
Configuration	auto-speed-auto-dup

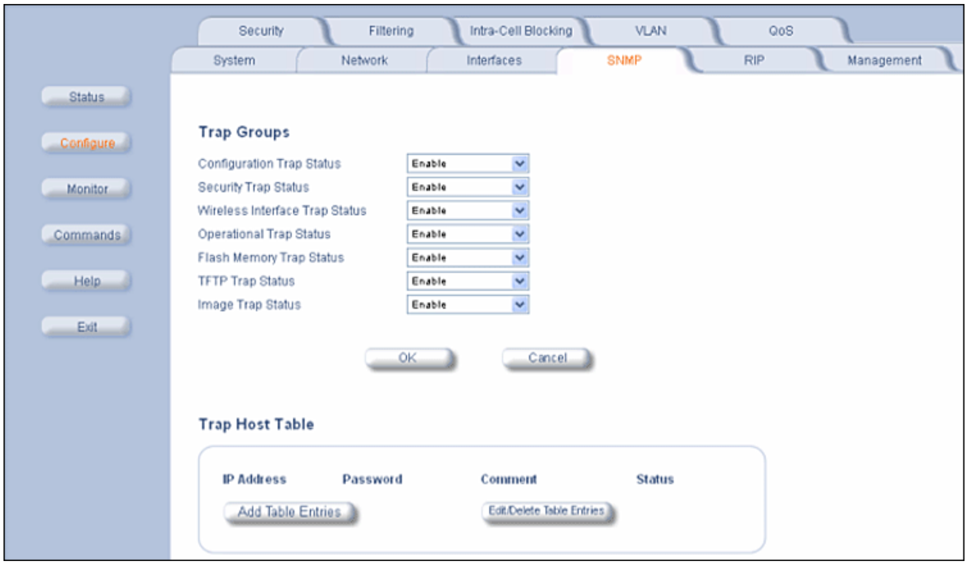
You can set the desired speed and transmission mode by clicking on **Configuration**. Select from these settings for the type of Ethernet transmission:

- **Half-duplex** means that only one side can transmit at a time.
- **Full-duplex** lets both sides transmit.
- **Auto-duplex** selects the best transmission mode available when both sides are set to auto-select.

The recommended setting is **auto-speed-auto-duplex**.

SNMP Parameters

Click **Configure** > **SNMP** to enable or disable trap groups, and to configure the SNMP management stations to which the unit sends system traps. See “Trap Groups” in the *Tsunami MP.11 Reference Manual* for a list of the system traps.

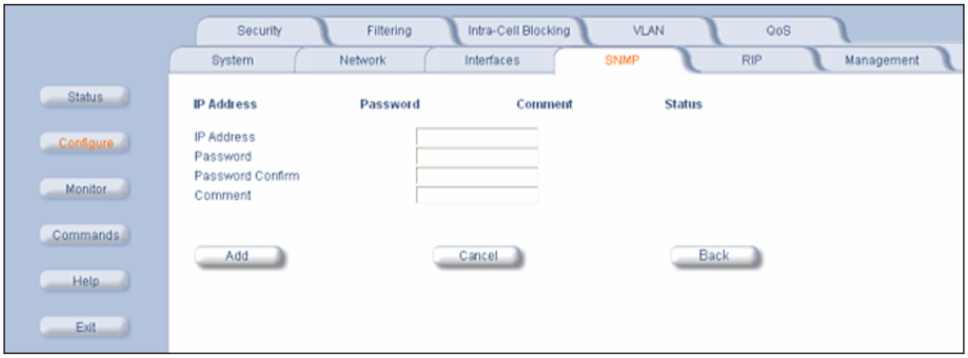


Configuration Trap Status	Enable
Security Trap Status	Enable
Wireless Interface Trap Status	Enable
Operational Trap Status	Enable
Flash Memory Trap Status	Enable
TFTP Trap Status	Enable
Image Trap Status	Enable

- **Trap Groups:** You can enable or disable different types of traps in the system. By default, all traps are enabled.
- **Trap Host Table:** This table shows the SNMP management stations to which the unit sends system traps.

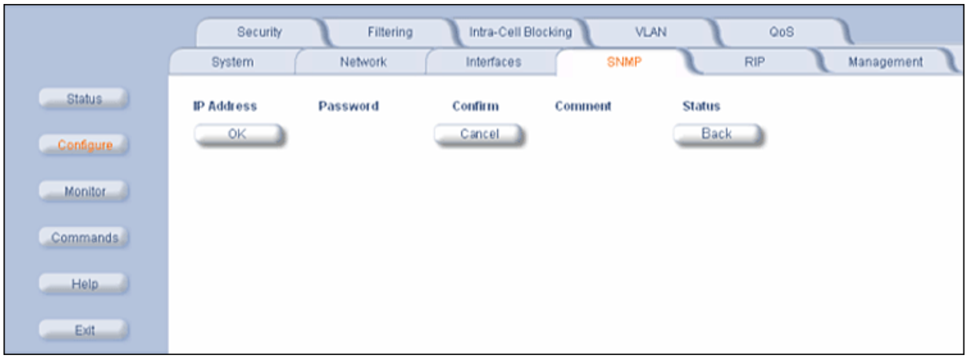
Add Entries to the Trap Host Table

Click the **Add Table Entries** button to add entries to the Trap Host Table.



Edit/Delete Entries to the Trap Host Table

Click the **Edit/Delete Table Entries** button to make changes to or delete existing entries.

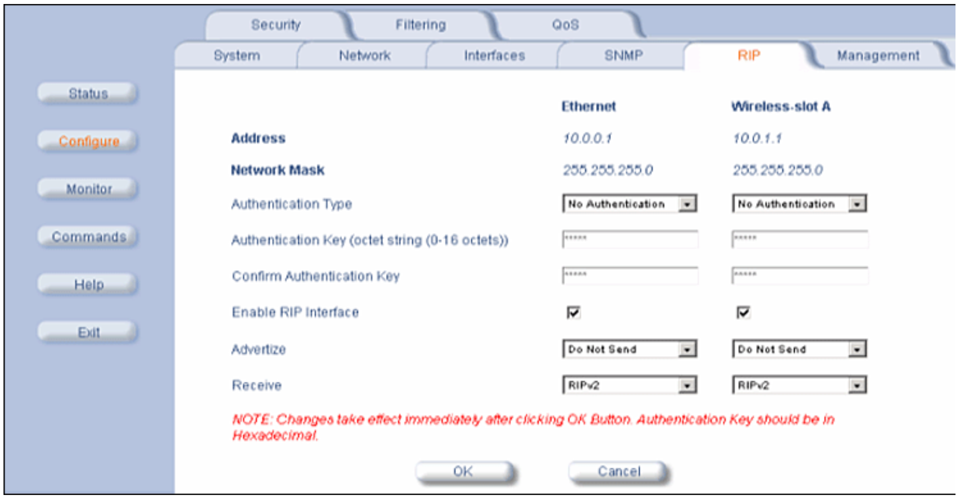


IP Address	Password	Confirm	Comment	Status

RIP Parameters

Routing Internet Protocol (RIP) is a dynamic routing protocol you can use to help automatically propagate routing table information between routers. The unit can be configured as RIPv1, RIPv2, RIPv1 Compatible, or a combination of the three versions while operating in **Routing** mode. In general, the unit's RIP module is based upon RFC 1389.

NOTE: *RIP does not work when Network Address Translation (NAT) is enabled.*



	Ethernet	Wireless-slot A
Address	10.0.0.1	10.0.1.1
Network Mask	255.255.255.0	255.255.255.0
Authentication Type	No Authentication	No Authentication
Authentication Key (octet string (0-16 octets))	*****	*****
Confirm Authentication Key	*****	*****
Enable RIP Interface	☑	☑
Advertize	Do Not Send	Do Not Send
Receive	RIPv2	RIPv2

NOTE: Changes take effect immediately after clicking OK Button. Authentication Key should be in Hexadecimal.

Note the following:

- RIPv2 is enabled by default when routing mode is selected.
- You may turn RIP off by clearing the **Enable RIP Interface** check box for the Ethernet or the wireless interface. Any RIP advertisements that are received on the designated interface are ignored. All other options on the page are dimmed.
- If the Enable RIP Interface check box is selected, the unit sends RIP requests and "listens" for RIP updates coming from RIP-enabled devices advertising on the network. You may configure the Receive field for RIPv1, RIPv2, or a combination of both. Although the unit receives and processes these updates, it does not further propagate these updates unless configured to advertise RIP. Again, you may configure the **Advertize** field for RIPv1, RIPv2, or a combination of both.
- The ability to enable or disable default route propagation is not user configurable. Once initialized, the unit uses its static default route and does not advertise this route in RIP updates. If another router on your network is configured to advertise its default route, this route overwrites the static default route configured on the unit. The unit then also propagates the new dynamic default route throughout the network.

Be aware that, once a dynamic default route is learned, it behaves just as any other dynamic route learned through RIP. This means if the device sending the default route stops sending RIP updates, the default route times out and the unit has no default route to the network. Workarounds for this condition include rebooting or re-entering a static default route. In general, the best approach is to disable the propagation of default routes on the other routers in your network unless you understand the risks.

The following table describes the properties and features of each version of RIP supported.

Properties and Features of Supported RIP Versions		
RIPv1	**RIPv2**	**RIPv1 Compatible**
Broadcast	Multicast	Broadcast
No Authentication	Authentication	Authentication
Class routing	Classless routing (VLSM)	Classless routing (VLSM)
Distance-vector protocol	Distance-vector protocol	Distance-vector protocol

Properties and Features of Supported RIP Versions		
RIPv1	**RIPv2**	**RIPv1 Compatible**
Metric-Hops	Metric-Hops	Metric-Hops
Maximum Distance 15	Maximum Distance 15	Maximum Distance 15
IGP	IGP	IGP

RIP Example

In the following example, assume that both the BSU and the SUs all are configured in **Routing** mode with RIP enabled to send and receive on both the Ethernet and Wireless interfaces. The network converges through updates until each unit has the following routing table:

BSU

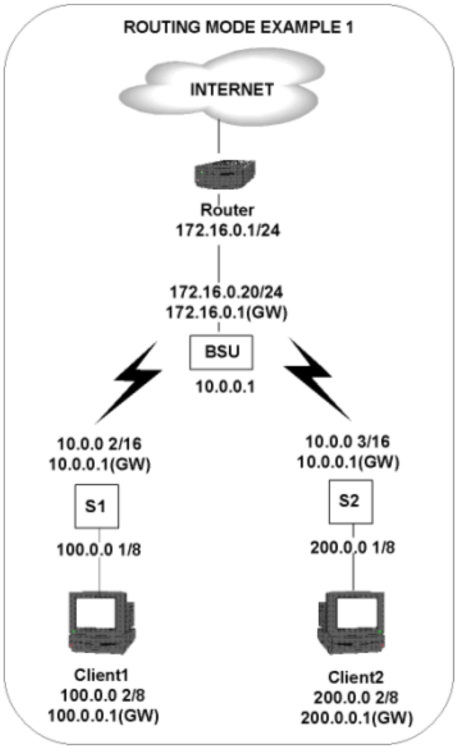
```
0.0.0.0        172.16.0.1    metric 1
172.16.0.0     172.16.0.20   metric 1
10.0.0.0       10.0.0.1      metric 1
100.0.0.0      10.0.0.2      metric 2
200.0.0.0      10.0.0.3      metric 2
```

SU1

```
0.0.0.0        10.0.0.1      metric 1
10.0.0.0       10.0.0.2      metric 1
100.0.0.0      100.0.0.1     metric 1
172.16.0.0     10.0.0.1      metric 2
200.0.0.0      10.0.0.2      metric 2
```

SU2

```
0.0.0.0        10.0.0.1      metric 1
10.0.0.0       10.0.0.3      metric 1
200.0.0.0      200.0.0.1     metric 1
172.16.0.0     10.0.0.1      metric 2
100.0.0.0      10.0.0.2      metric 2
```



RIP Notes

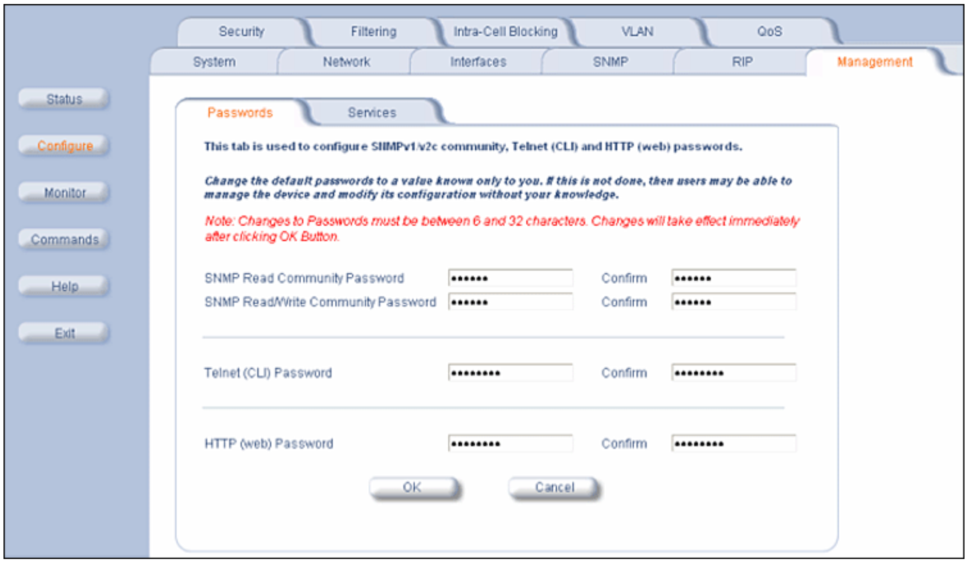
- Ensure that routers on the same physical network are configured to use the same version of RIP.
- Routing updates occur every 30 seconds. It may take up to 3 minutes for a route that has gone down to timeout in a routing table.
- RIP is limited to networks with 15 or fewer hops.

Management Parameters

When you click the **Management** button, Passwords is displayed automatically. The other tab under **Management** is the **Services** tab.

Configure Passwords

The **Password** tab lets you configure the SNMP, Telnet, and HTTP (Web Interface) passwords.



This tab is used to configure SIIMPv1/v2c community, Telnet (CLI) and HTTP (web) passwords.

Change the default passwords to a value known only to you. If this is not done, then users may be able to manage the device and modify its configuration without your knowledge.

Note: Changes to Passwords must be between 6 and 32 characters. Changes will take effect immediately after clicking OK Button.

SNMP Read Community Password: •••••• Confirm: ••••••
SNMP Read/Write Community Password: •••••• Confirm: ••••••

Telnet (CLI) Password: ••••••••• Confirm: •••••••••

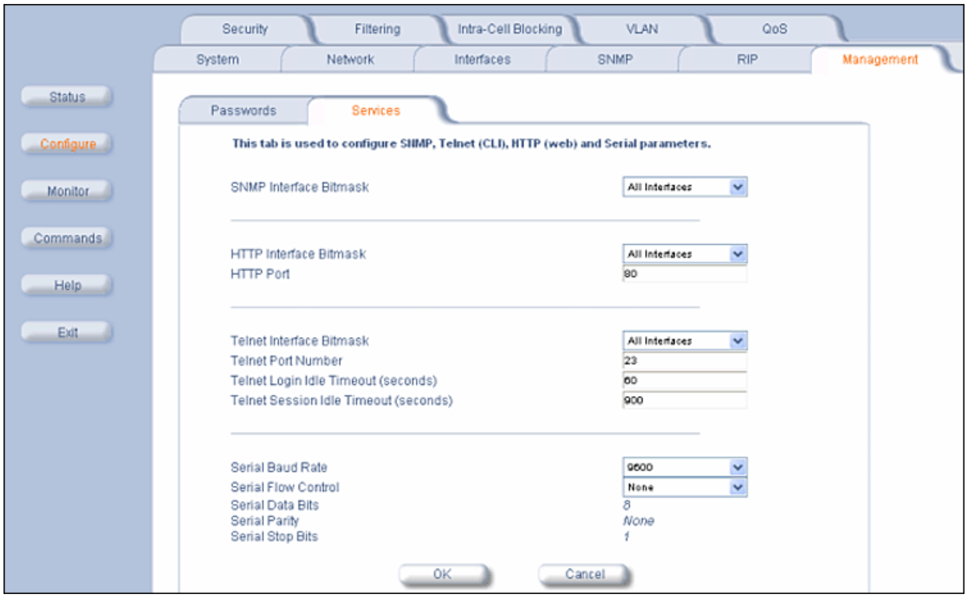
HTTP (web) Password: ••••••••• Confirm: •••••••••

For all password fields, the passwords must be between 6 and 32 characters. Changes take effect immediately after you click **OK**. The following passwords are configurable:

- **SNMP Read Community Password:** The password for read access using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **SNMP Read/Write Community Password:** The password for read and write access using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **Telnet (CLI) Password:** The password for the CLI interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **HTTP (Web) Password:** The password for the Web browser HTTP interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.

Configure Service Parameters

The **Services** tab lets you configure the SNMP, Telnet, and HTTP (Web Interface) parameters. Changes to these parameters require a reboot to take effect.



This tab is used to configure SNMP, Telnet (CLI), HTTP (web) and Serial parameters.

SNMP Interface Bitmask	All Interfaces
HTTP Interface Bitmask	All Interfaces
HTTP Port	80
Telnet Interface Bitmask	All Interfaces
Telnet Port Number	23
Telnet Login Idle Timeout (seconds)	60
Telnet Session Idle Timeout (seconds)	900
Serial Baud Rate	9600
Serial Flow Control	None
Serial Data Bits	8
Serial Parity	None
Serial Stop Bits	1

SNMP Configuration Settings

- **SNMP Interface Bitmask:** Configure the interface or interfaces (**Ethernet**, **Wireless**, **All Interfaces**) from which you will manage the unit using SNMP. You also can select **Disabled** to prevent a user from accessing the unit through SNMP.

HTTP Configuration Settings

- **HTTP Interface Bitmask:** Configure the interface or interfaces (**Ethernet**, **Wireless**, **All Interfaces**) from which you will manage the unit through the Web interface. For example, to allow Web configuration through the Ethernet network only, set **HTTP Interface Bitmask** to **Ethernet**. You can also select **Disabled** to prevent a user from accessing the unit from the Web interface.
- **HTTP Port:** Configure the HTTP port from which you will manage the unit through the Web interface. By default, the HTTP port is 80.

Telnet Configuration Settings

NOTE: *To use HyperTerminal for CLI access, make sure to check “Send line ends with line feeds” in the ASCII Setup window (in the HyperTerminal window, click Properties; then select Setup > ASCII Setup. See “HyperTerminal Connection Properties” in the Tsunami MP.11 Reference Manual for more information).*

- **Telnet Interface Bitmask:** Select the interface (Ethernet, Wireless, All Interfaces) from which you can manage the unit through telnet. This parameter can also be used to disable telnet management.
- **Telnet Port Number:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select).
- **Telnet Login Timeout** (seconds): Enter the number of seconds the system is to wait for a login attempt. The unit terminates the session when it times out. The range is 1 to 300 seconds; the default is 30 seconds.
- **Telnet Session Timeout** (seconds): Enter the number of seconds the system is to wait during a session while there is no activity. The unit ends the session upon timeout. The range is 1 to 36000 seconds; the default is 900 seconds.

Serial Configuration Settings

The serial port interface on the unit is enabled at all times. See “Serial Port” in the *Tsunami MP.11 Reference Manual* for information about how to access the CLI interface through the serial port. You can configure and view following parameters:

- **Serial Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.
- **Serial Flow Control:** Select either None (default) or Xon/Xoff (software controlled) data flow control. To avoid potential problems when communicating with the unit through the serial port, Proxim recommends that you leave the Flow Control setting at None (the default value).
- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

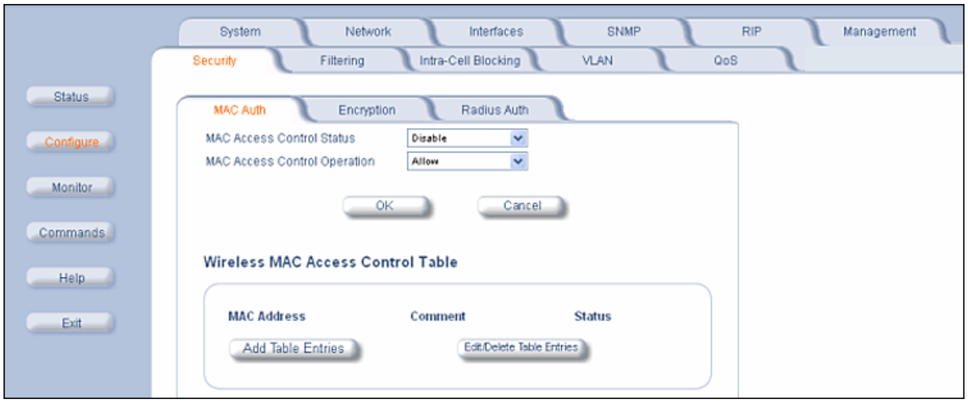
The serial port bit configuration is commonly referred to as 8N1.

Security Parameters

Configure MAC Authentication

Click **Configure** > **Security** > **MAC Auth** to build a list of authorized wireless stations that can register at the unit and access the network.

MAC authentication is available only for BSUs.



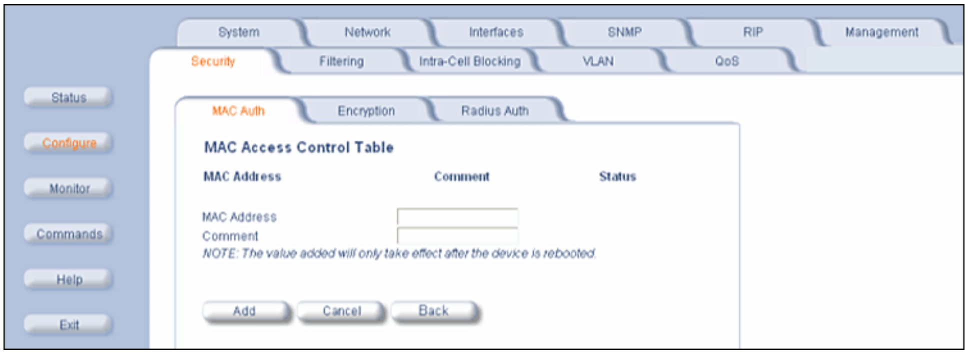
MAC Access Control Status: Disable
MAC Access Control Operation: Allow

Wireless MAC Access Control Table

MAC Address	Comment	Status

This feature is supported on the wireless interface and only wireless MAC addresses should be entered in the list. For example, build a list of wireless MAC addresses on the BSU for the authorized SUs.

To add table entries, click the **Add Table Entries** button; a window such as the following is displayed:



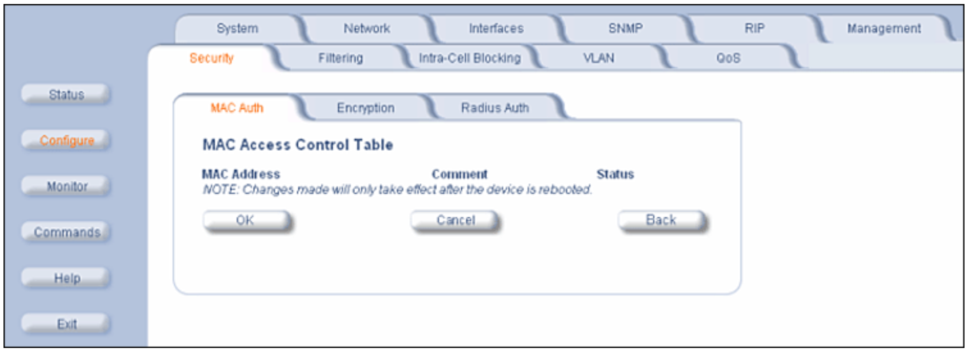
MAC Access Control Table

MAC Address	Comment	Status

MAC Address
Comment
NOTE: The value added will only take effect after the device is rebooted.

Enter the MAC address and any comment, then click **Add**. The maximum number of MAC addresses that can be entered is 250.

To edit or delete table entries, click the **Edit/Delete Table Entries** button; make your corrections in the window displayed and click **OK**.



MAC Access Control Table

MAC Address	Comment	Status

NOTE: Changes made will only take effect after the device is rebooted.

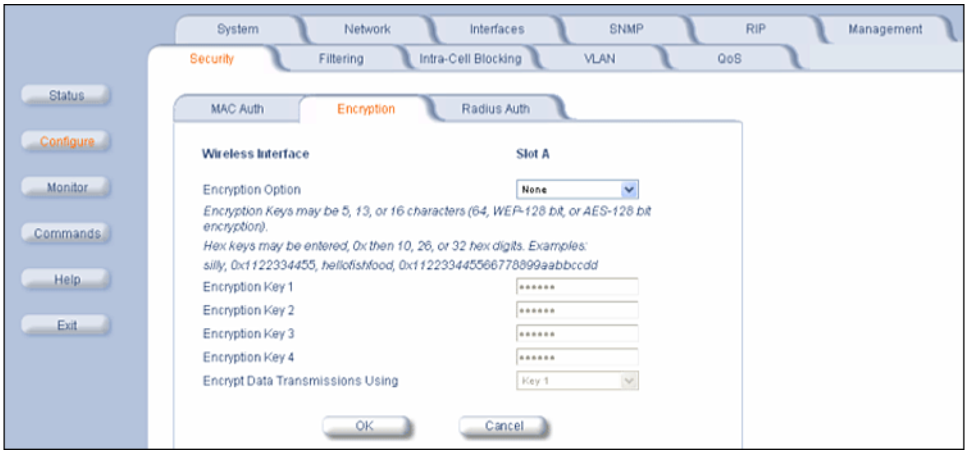
Configure Encryption Parameters

NOTE: *Be sure to set the encryption parameters and change the default passwords.*

You can protect the wireless data link by using encryption. Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values.

In addition to Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP), the unit supports Advanced Encryption Standard (AES) 128-bit encryption. To provide even stronger encryption, the AES CCM Protocol is also supported.

Click **Configure** > **Security** > **Encryption** to set encryption keys for the data transmitted and received by the unit. Note that all devices in one network must use the same encryption parameters to communicate to each other.



Wireless Interface	**Slot A**
Encryption Option	None

Encryption Keys may be 5, 13, or 16 characters (64, WEP-128 bit, or AES-128 bit encryption).

Hex keys may be entered, 0x then 10, 26, or 32 hex digits. Examples:

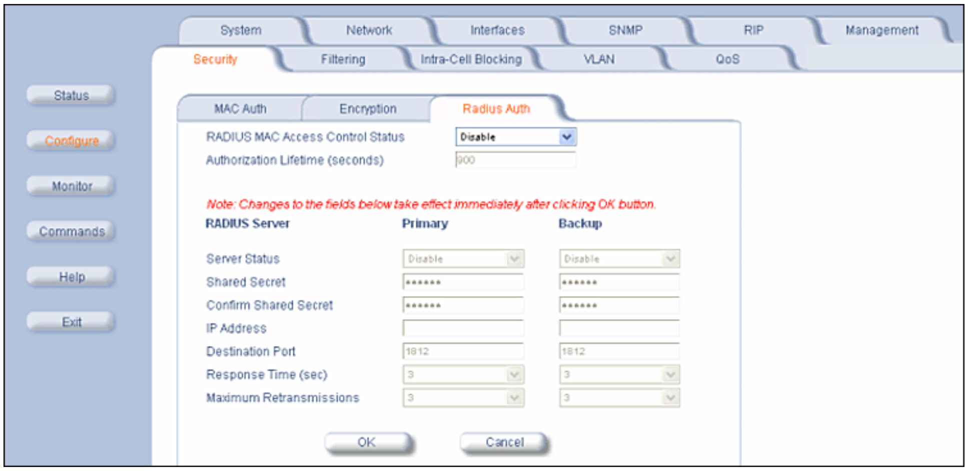
silly, 0x1122334455, hellofishfood, 0x112233445566778899aabbccdd

Encryption Key 1	******
Encryption Key 2	******
Encryption Key 3	******
Encryption Key 4	******
Encrypt Data Transmissions Using	Key 1

Configure RADIUS Authentication

Click **Configure** > **Security** > **Radius Auth** to set the IP address of the RADIUS server containing the central list of MAC addresses that are allowed to access the network. The RADIUS parameters let you enable HTTP or Telnet RADIUS management access to configure a RADIUS Profile for management access control, to enable or disable local user access, and to configure the local password.

RADIUS authentication is available only for BSUs.



RADIUS MAC Access Control Status: Disable
Authorization Lifetime (seconds): 900

Note: Changes to the fields below take effect immediately after clicking OK button.

RADIUS Server	**Primary**	**Backup**
Server Status	Disable	Disable
Shared Secret	******	******
Confirm Shared Secret	******	******
IP Address		
Destination Port	1812	1812
Response Time (sec)	3	3
Maximum Retransmissions	3	3

In large networks with multiple units, you can maintain a list of MAC addresses on a centralized location using a RADIUS authentication server that grants or denies access. If you use this kind of authentication, you must specify at least the primary RADIUS server. The backup RADIUS server is optional.

Filtering Parameters

Click **Configure** > **Filtering** to configure packet filtering. Packet filtering can be used to control and optimize network performance.

Overview

The Filtering feature can selectively filter specific packets based upon their Ethernet protocol type. Protocol filtering is done at the Bridge layer.

Protocol filters are useful for preventing bridging of selected protocol traffic from one segment of a network to other segments (or subnets). You can use this feature both to increase the amount of bandwidth available on your network and to increase network security.

Increasing Available Bandwidth

It may be unnecessary to bridge traffic from a subnet using IPX/SPX or AppleTalk to a segment of the network with UNIX workstations. By denying the IPX/SPX AppleTalk traffic from being bridged to the UNIX subnet, the UNIX subnet is free of this unnecessary traffic.

Increasing Network Security

By bridging IP and IP/ARP traffic and blocking LAN protocols used by Windows, Novell, and Macintosh servers, you can protect servers and client systems on the private local LAN from outside attacks that use those LAN protocols. This type of filtering also prevents private LAN data from being bridged to an untrusted remote network or the Internet.

To prevent blocking your own access (administrator) to the unit, Proxim recommends that IP (0x800) and ARP (0x806) protocols are always passed through.

Sample Use and Validation

Configure the protocol filter to let only IP and ARP traffic pass through the unit (bridge) from one network segment to another. Then, attempt to use Windows file sharing across the bridge. The file should not allow sharing; the packets are discarded by the bridge.

Setting the ARP Filter

There may be times when you need to set the ARP or Multicast. Usually, this is required when there are many nodes on the wired network that are sending ARP broadcast messages or multicast packets that unnecessarily consume the wireless bandwidth. The goal of these filters is to allow only necessary ARP and multicast traffic through the 1.6 Mbps wireless pipe.

The TCP/IP Internet Protocol Suite uses a method known as ARP (Address Resolution Protocol) to match a device's MAC (Media Access Control) address with its assigned IP address. The MAC address is a unique 48-bit identifier assigned to each hardware device at the factory by the manufacturer. The MAC address is commonly represented as 6 pairs of hexadecimal digits separated by colons. For example, a device may have the MAC address of 00:20:A6:33:ED:45.

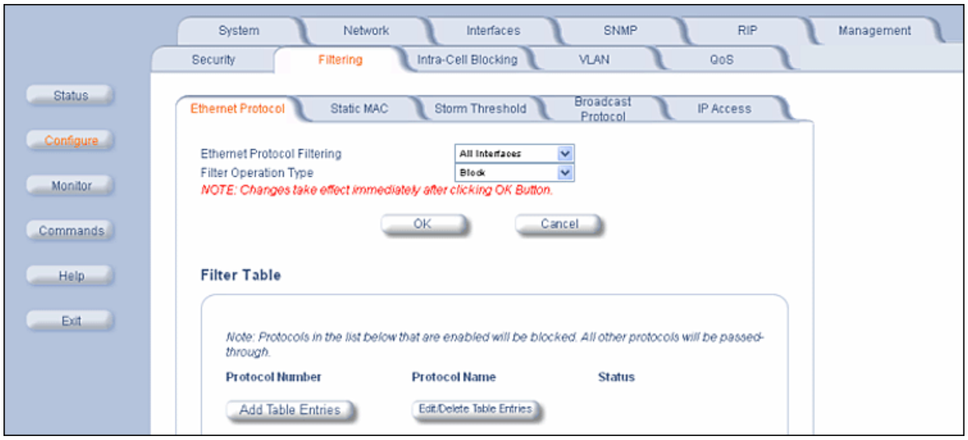
When devices send data over the network (Ethernet, Token Ring, or wireless), they use the MAC address to identify a packet's source and destination. Therefore, an IP address must be mapped to a MAC address in order for a device to send a packet to particular IP address. In order to resolve a remote node's IP address with its MAC address, a device sends out a broadcast packet to all nodes on the network. This packet is known as an ARP request or ARP broadcast and requests that the device assigned a particular IP address respond to the sender with its MAC address.

Because ARP requests are broadcast packets, these packets are forwarded to wireless nodes by default, even if the packet is not meant for a wireless node. As the number of nodes on a network backbone increases, so does the number of ARP broadcasts that are forwarded to the wireless nodes. Many of these ARP broadcasts are unnecessary and can consume valuable wireless bandwidth. On some networks, there are so many ARP broadcasts that the performance of the wireless network will degrade due to the amount of bandwidth being consumed by these messages.

To reduce the number of ARP broadcasts that are forwarded to the wireless nodes, you can enable ARP filtering. When enabled, the ARP Filter allows the unit to forward only those ARP broadcasts destined for an IP address that falls within the range specified by the ARP Filter Network Address and the ARP Filter Subnet Mask. The ARP Filter performs a logical AND function (essentially keeping what is the same and discarding what is different) on the IP address of the ARP request and the ARP Filter Subnet Mask. It then compares the result of the logical AND to the ARP Filter Network Address. If the two values match, the ARP broadcast is forwarded to the wireless network by the unit.

Configure Ethernet Protocol Filtering

The Ethernet Protocol filter blocks or forwards packets based upon the Ethernet protocols they support. Click **Configure** > **Filtering** > **Ethernet Protocol** to enable or disable certain protocols in the table. Entries can be selected from a drop-down box.



Ethernet Protocol Filtering: All Interfaces
Filter Operation Type: Block
NOTE: Changes take effect immediately after clicking OK Button.

Filter Table

Note: Protocols in the list below that are enabled will be blocked. All other protocols will be passed-through.

Protocol Number	Protocol Name	Status

Follow these steps to configure the Ethernet Protocol Filter:

1. Select the interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
   - Ethernet: Packets are examined at the Ethernet interface
   - Wireless-Slot A or Wireless-Slot B: Packets are examined at the Wireless A or B interfaces
   - All Interfaces: Packets are examined at both interfaces
   - Disabled: The filter is not used
2. Select the **Filter Operation Type**.
   - If set to Block, the bridge blocks enabled Ethernet Protocols listed in the Filter Table.
   - If set to Passthru, only the enabled Ethernet Protocols listed in the Filter Table pass through the bridge.
3. Configure the **Filter Table**.
   - To add an entry, click **Add Table Entries.** You may add one of the supplied Ethernet Protocol Filters, or you may enter additional filters by specifying the appropriate parameters:
     – To add one of the supplied Ethernet Protocol Filters to the filter table:
       - Select the appropriate filter from the **Specify Common Protocol** drop-down menu. Protocol Name and Protocol Number fields will be filled in automatically.
       - Click **Add**
     – To add a new filter to the filter table:
       - Enter the **Protocol Number**. See http://www.iana.org/assignments/ethernet-numbers for a list of protocol numbers.
       - Enter the Protocol Name.

  - Click **Add**.
- To edit or delete an entry, click **Edit** and change the information, or select Enable, Disable, or Delete from the Status drop-down menu.

  NOTE: *Entries must be enabled in order to be subject to the filter.*

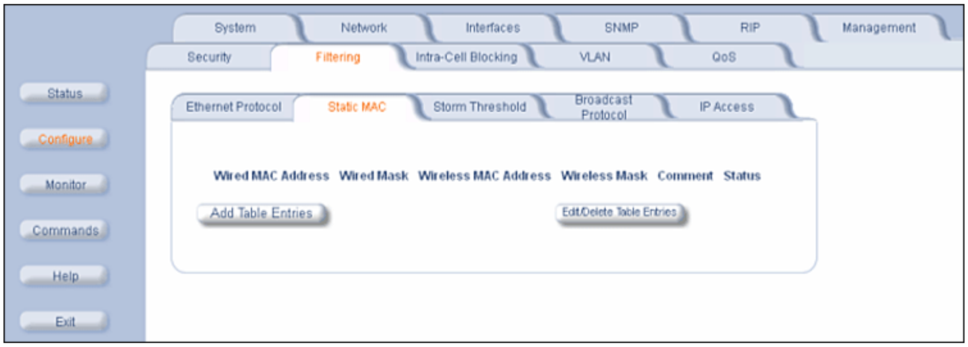
Configure Static MAC Pair Filtering

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. When this feature is configured properly, the unit can block traffic between wired devices on the wired (Ethernet) interface and devices on the wireless interface based upon MAC address.

NOTE: *The device on the wireless interface can be any device connected through the link, it can be directly connected to the Ethernet interface of the peer unit, or it can be attached through multiple hops. The MAC address in the packets arriving at the wireless interface is the important element.*

The filter is an advanced feature that lets you limit the data traffic between two specific devices (or between groups of devices based upon MAC addresses and masks) through the unit's wireless interface. For example, if you have a server on your network with which you do not want wireless clients to communicate, you can set up a static MAC filter to block traffic between these devices. The Static MAC Filter Table performs bi-directional filtering. However, note that this is an advanced filter and it may be easier to control wireless traffic through other filter options, such as **Protocol Filtering**.

Click **Configure** > **Filtering** > **Static MAC** to access the Static MAC Address filter.



Each MAC address or mask is comprised of 12 hexadecimal digits (0-9 and A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (0 or 1).

Taken together, a MAC address/mask pair specifies an address or a range of MAC addresses that the unit looks for when examining packets. The unit uses Boolean logic to perform an "and" operation between the MAC address and the mask at the bit level. However, for most users, you do not need to think in terms of bits. It should be sufficient to create a filter using only the hexadecimal digits 0 and F in the mask (where 0 is any value and F is the value specified in the MAC address). A mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a mask of FF:FF:FF:FF:FF:FF:FF:FF applies only to the specified MAC address.

For example, if the MAC address is 00:20:A6:12:54:C3 and the mask is FF;FF;FF;00:00:00, the unit examines the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the mask is FF;FF;FF;FF;FF;FF, the unit looks only for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, you can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters. Which parameters to configure depends upon the traffic that you want to block:

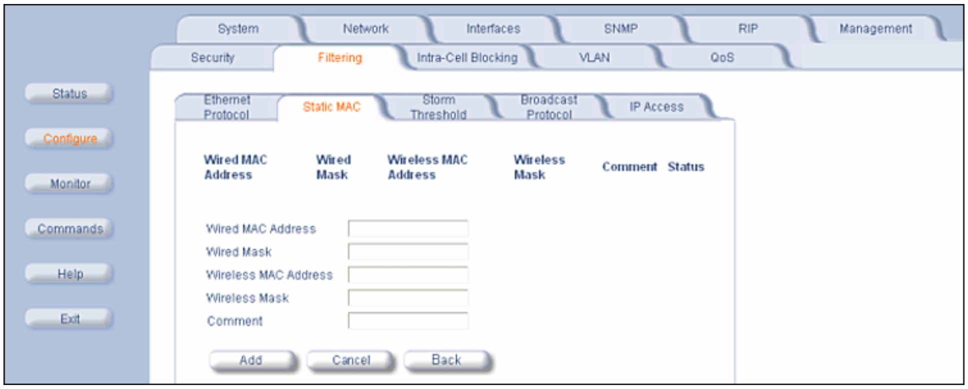
- To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC address and Wired mask (leave the Wireless MAC and Wireless mask set to all zeros).
- To prevent all traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC and Wireless mask (leave the Wired MAC address and Wired mask set to all zeros).

- To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

See Static MAC Filter Examples for more detailed examples.

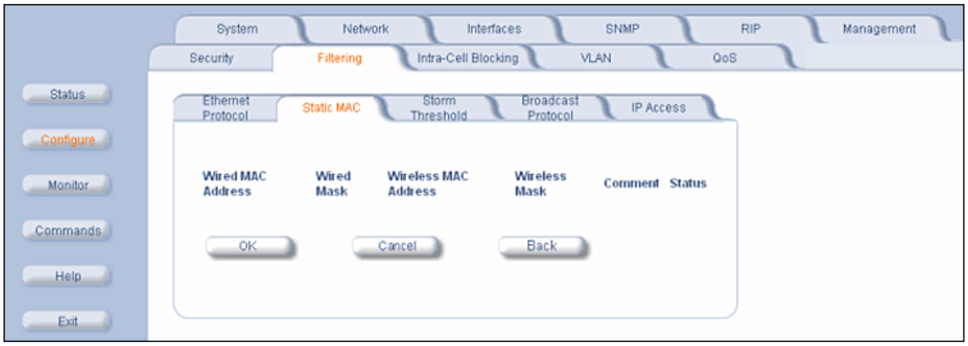
Add Entries to the Static MAC Filter Table

To add the entries to Filter table, click the **Add Table Entries** button.



After entering the data, click the **Add** button. The entry is enabled automatically when saved.

To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.



The following fields are may be configured or viewed:

- **Wired MAC Address:** Enter the MAC address of the device on the Ethernet network that you want to prevent from communicating with a device on the wireless network.
- **Wired Mask:** Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wired MAC Address field, enter 00:00:00:00:00:00 (all zeroes).
- **Wireless MAC Address:** Enter the MAC address of the wireless device on the wireless interface that you want to prevent from communicating with a device on the wired network.
- **Wireless Mask:** Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wireless MAC Address field, enter 00:00:00:00:00:00 (all zeroes).
- **Comment:** Enter related information.
- **Status:** The Status field can show **Enable**, **Disable**, or **Delete**.

Static MAC Filter Examples

Consider a network that contains a wired server and three wireless clients. The MAC address for each unit is as follows:

- **Wired Server:** 00:40:F4:1C:DB:6A
- **Wireless Client 1:** 00:02:2D:51:94:E4
- **Wireless Client 2:** 00:02:2D:51:32:12
- **Wireless Client 3:** 00:20:A6:12:4E:38

Prevent two specific devices from communicating:

Configure the following settings to prevent the Wired Server and Wireless Client 1 from communicating:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: Traffic between the Wired Server and Wireless Client 1 is blocked. Wireless Clients 2 and 3 still can communicate with the Wired Server.

Prevent Multiple Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:00:00:00

Result: When a logical "AND" is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Server and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Server since it has a different prefix (00:20:A6).

Prevent All Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent all three Wireless Clients from communicating with Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The unit blocks all traffic between the Wired Server and all wireless clients.

Prevent A Wireless Device From Communicating With the Wired Network

Configure the following settings to prevent Wireless Client 3 from communicating with any device on the Ethernet:

- **Wired MAC Address:** 00:00:00:00:00:00
- **Wired Mask:** 00:00:00:00:00:00
- **Wireless MAC Address:** 00:20:A6:12:4E:38
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: The unit blocks all traffic between Wireless Client 3 and the Ethernet network.

Prevent Messages Destined for a Specific Multicast Group from Being Forwarded to the Wireless LAN

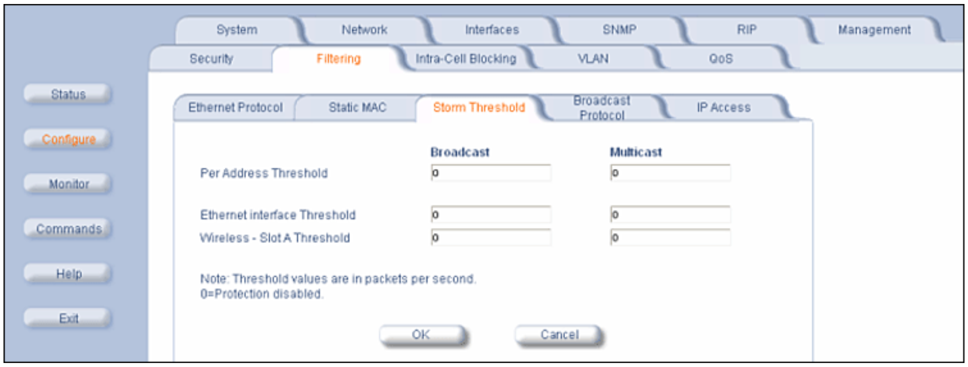
If devices on your Ethernet network use multicast packets to communicate and these packets are not required by your wireless clients, you can set up a Static MAC filter to preserve wireless bandwidth. For example, if routers on your network use a specific multicast address (such as 01:00:5E:00:32:4B) to exchange information, you can set up a filter to prevent these multicast packets from being forwarded to the wireless network:

- **Wired MAC Address:** 01:00:5E:00:32:4B
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The unit does not forward any packets that have a destination address of 01:00:5E:00:32:4B to the wireless network.

Configure Storm Threshold Filtering

Click **Configure** > **Filtering** > **Storm Threshold** to use threshold limits to prevent broadcast/multicast overload.



	Broadcast	Multicast
Per Address Threshold	0	0
Ethernet interface Threshold	0	0
Wireless - Slot A Threshold	0	0

Note: Threshold values are in packets per second.
0=Protection disabled.

Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by specifying:

- A maximum number of frames per second as received from a single network device (identified by its MAC address).
- An absolute maximum number of messages per port.

The **Storm Threshold** parameters let you specify a set of thresholds for each port of the unit, identifying separate values for the number of broadcast messages per second and multicast messages per second.

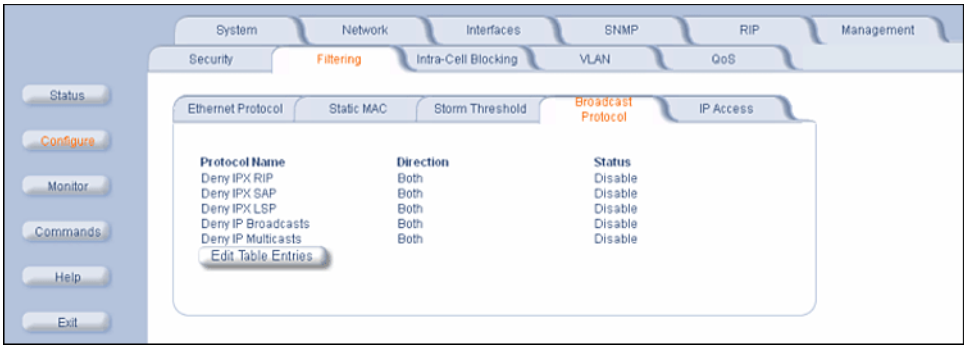
When the number of frames for a port or identified station exceeds the maximum value per second, the unit ignores all subsequent messages issued by the particular network device, or ignores all messages of that type.

The following parameters are configurable:

- **Per Address Threshold:** Enter the maximum allowed number of packets per second.
- **Ethernet Threshold:** Enter the maximum allowed number of packets per second.
- **Wireless Threshold:** Enter the maximum allowed number of packets per second.

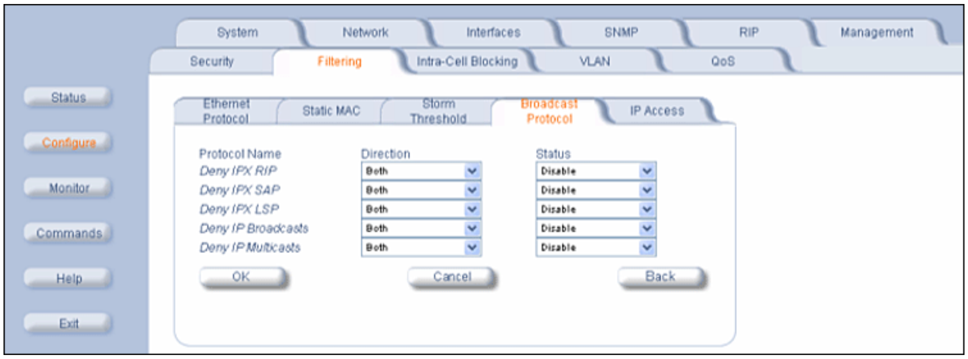
Configure Broadcast Protocol Filtering

Click **Configure** > **Filtering** > **Broadcast Protocol** to deny specific IP broadcast, IPX broadcast, and multicast traffic.



Protocol Name	Direction	Status
Deny IPX RIP	Both	Disable
Deny IPX SAP	Both	Disable
Deny IPX LSP	Both	Disable
Deny IP Broadcasts	Both	Disable
Deny IP Multicasts	Both	Disable

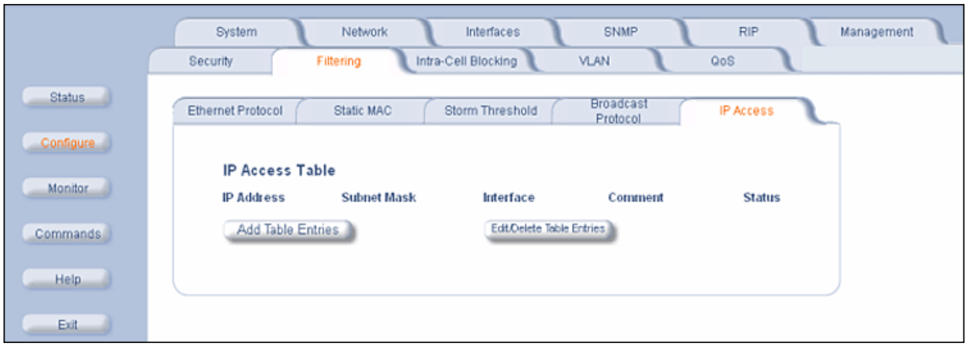
Click the **Edit Table Entries** button to display an editable window such as the following. You can configure whether this traffic must be blocked for Ethernet to wireless, wireless to Ethernet, or both.



Protocol Name	Direction	Status
Deny IPX RIP	Both	Disable
Deny IPX SAP	Both	Disable
Deny IPX LSP	Both	Disable
Deny IP Broadcasts	Both	Disable
Deny IP Multicasts	Both	Disable

Configure IP Access Table Filtering

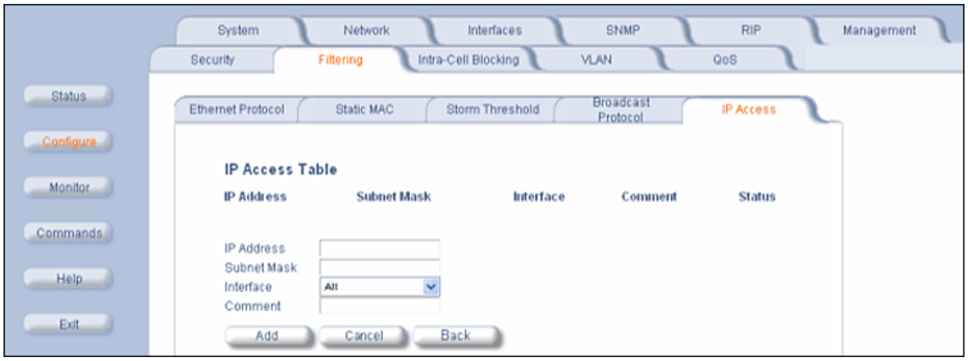
Click **Configure** > **Filtering** > **IP Access Table** to limit in-band management access to the IP addresses or range of IP addresses specified in the table. This feature applies to all management services (SNMP, HTTP, and CLI), except for CLI management over the serial port.



IP Access Table

IP Address	Subnet Mask	Interface	Comment	Status

To add an entry, click the **Add Table Entries** button, specify the IP address and mask of the wireless stations to which you want to grant access, and click **Add**.

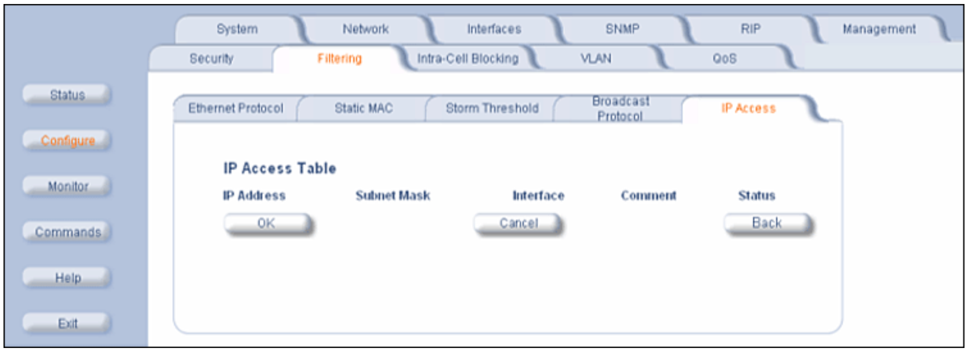


IP Access Table

IP Address	Subnet Mask	Interface	Comment	Status

IP Address
Subnet Mask
Interface: All
Comment

To edit or delete table entries, click the **Edit/Delete Table Entries** button, make your changes, and click **OK**.



IP Access Table

IP Address	Subnet Mask	Interface	Comment	Status

For example, **172.17.23.0/255.255.255.0** allows access from all wireless stations with an IP address in the 172.17.23.xxx range.

Ensure that the IP address of the management PC you use is within the first entry in the table, as this filter takes effect immediately. Otherwise, you have locked yourself out.

When you do lock yourself out, you may try to give the PC the correct IP address; otherwise you must reset the unit.

Intra-Cell Blocking (Base Station Unit only)

Overview

The Intra-Cell Blocking feature lets traffic be blocked between two SUs registered to the same Base Station. There are two potential reasons to isolate traffic among wireless subscribers:

- To provide better security to the subscribers by isolating the traffic from one subscriber to another in a public space.
- To block unwanted traffic between subscribers to prevent this traffic from using bandwidth.

You can form groups of SUs at the Base Station, which define the filtering criteria. All data to or from SUs belonging to the same group are bridged. All other data from SUs that do not belong to a particular group are automatically forwarded through the Ethernet interface of the Base Station. If an SU does not belong to any group, the Base Station discards the data.

You can also configure a *Security Gateway* to block traffic between SUs connected to different BSUs. All packets destined for SUs not connected to the same Base Station are forwarded to the Security Gateway MAC address (configured in the *Security Gateway* tab).

When you change the device from **Bridge** to **Routing** mode, Intra-Cell Blocking stops working with or without a reboot. When you change the device from **Routing** to **Bridge** mode, Intra-Cell Blocking starts working with or without a reboot.

Intra-Cell Blocking Group Rules

The following rules apply to Intra-Cell Blocking Groups:

- One SU can be assigned to more than one group.
- An SU that has not been assigned to any group cannot communicate to any other SU connected to the same or different BSU.

Example of Intra-Cell Blocking Groups

Assume that four Intra-Cell Blocking Groups have been configured on one BSU. SUs 1 through 6 are registered to BSU 1. SUs 7 through 9 are registered to BSU 2.

Intra-Cell Blocking Group Example			
Group 1	**Group 2**	**Group 3**	**Group 4**
SU 1	SU 2	SU 6	SU 8
SU 4	SU 3	SU 1	SU 9
SU 5	SU 8	SU 3	SU 2

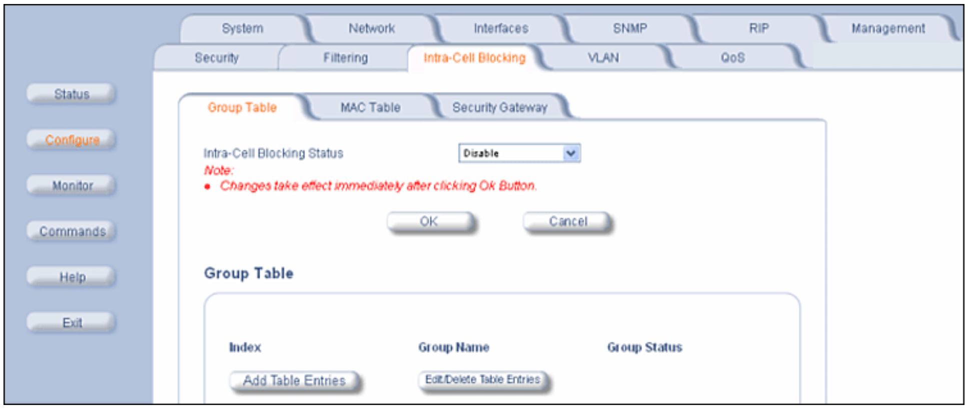
In this example, SU 1 belongs to two groups, Group 1 and Group 3. Therefore, packets from SU 1 destined to SU 4, SU 5, SU 6, and SU 3 are not blocked. However, SU 9 belongs to group 4 only and packets from SU 9 are blocked unless sent to SU 8 or SU 2.

Achieving Communication Between Two SUs

In a multipoint configuration, an SU can communicate with another SU through the BSU when in Bridge mode by default. Use the intra-cell blocking feature if this is not desired. In a routing configuration, each of the SUs must have a different subnet on their Ethernet port to distinguish traffic for each SU, and each subnet must be entered into a routing rule in the BSU as well as into an upstream router. The wireless side of all SUs must share the same subnet with the BSU wireless interface. These IP addresses must be used as next hop when creating the routes for the SU subnets.

Enable Intra-Cell Blocking

Click **Configure** > **Intra-Cell Blocking** > **Group Table** to enable the Intra-Cell Blocking feature and to configure Intra-Cell Blocking Groups.



Intra-Cell Blocking Status: Disable

Note:

- *Changes take effect immediately after clicking Ok Button.*

Group Table

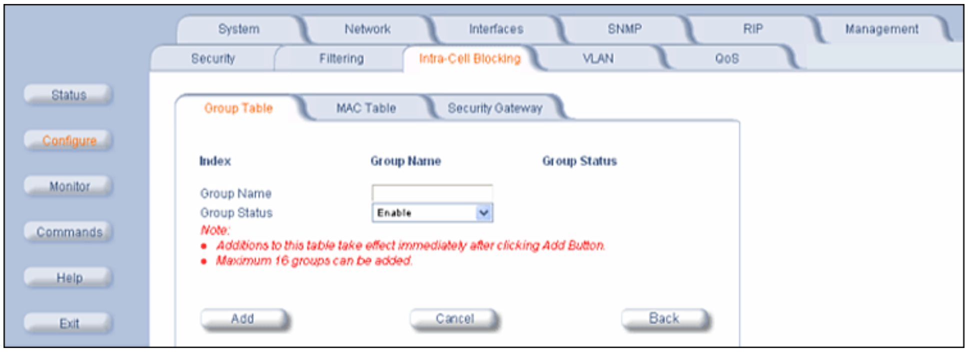
Index	Group Name	Group Status

The following items are configurable:

- **Intra-Cell Blocking Status:** Enables or disables the Intra-Cell Blocking feature.
- **Group Table:** Entries in this table show the Intra-Cell Blocking filter groups that have been configured. When Intra-Cell Blocking is enabled, the Base Station Unit discards all packets coming from one SU to another SU, if both SUs do not belong to the same filter group.

Configure Intra-Cell Blocking Groups

Click the **Add Table Entries** button to add groups to the Group Table.



Index	Group Name	Group Status

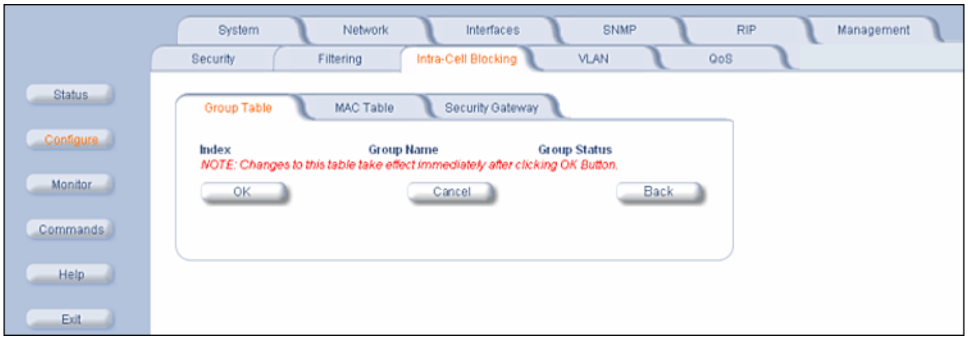
Group Name:
Group Status: Enable

Note:

- *Additions to this table take effect immediately after clicking Add Button.*
- *Maximum 16 groups can be added.*

Enter the group name, and click **Add**. The group is assigned an Index and appears in the Group Table. Up to 16 groups can be configured per Base Station.

You can enable, disable or delete an existing filter group by using the **Edit/Delete Table Entries** button.

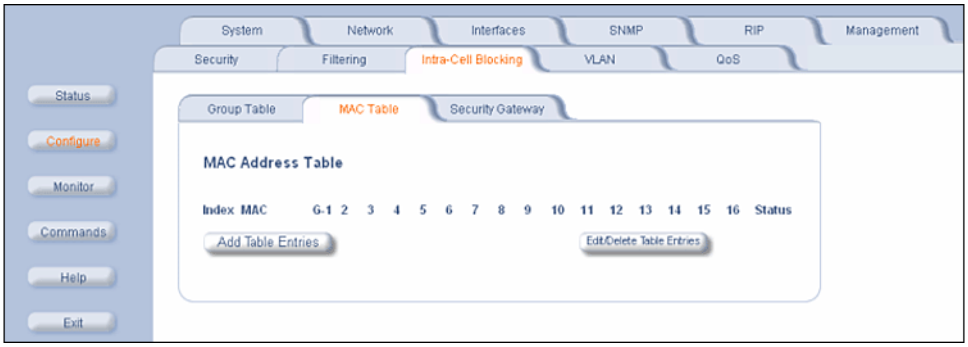


Index Group Name Group Status

NOTE: Changes to this table take effect immediately after clicking OK Button.

Assign MAC Addresses (MAC Table)

After configuring the Intra-Cell Blocking Groups on the **Group Table** tab, use the **MAC Table** tab to assign specific MAC addresses to an Intra-Cell Blocking Group.

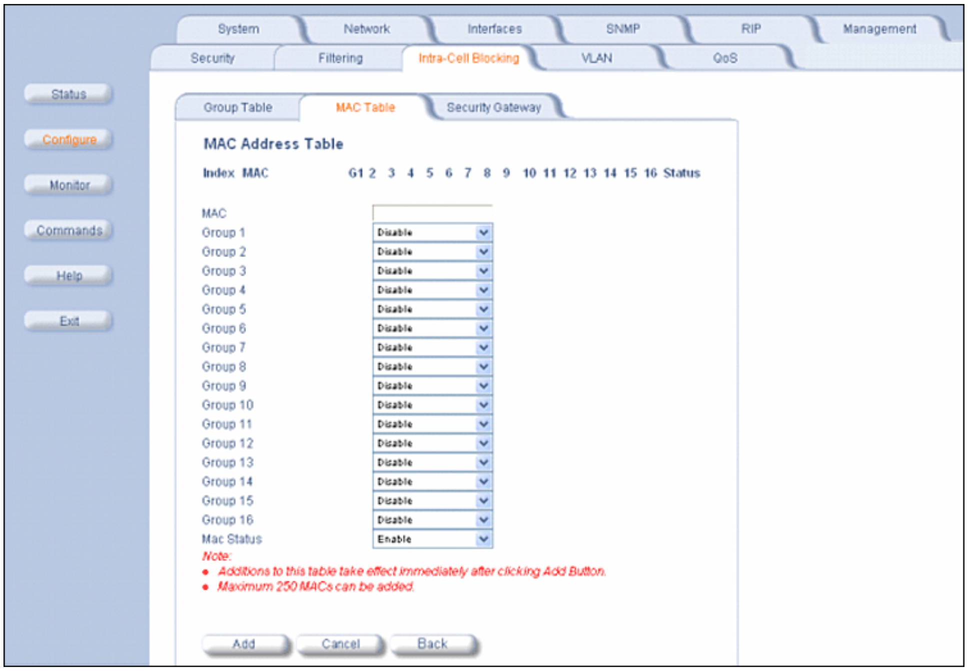


MAC Address Table

Index	MAC	G-1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Status

Adding Entries

Click the **Add Table Entries** button.



MAC Address Table

Index	MAC	G1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Status

MAC	
Group 1	Disable
Group 2	Disable
Group 3	Disable
Group 4	Disable
Group 5	Disable
Group 6	Disable
Group 7	Disable
Group 8	Disable
Group 9	Disable
Group 10	Disable
Group 11	Disable
Group 12	Disable
Group 13	Disable
Group 14	Disable
Group 15	Disable
Group 16	Disable
Mac Status	Enable

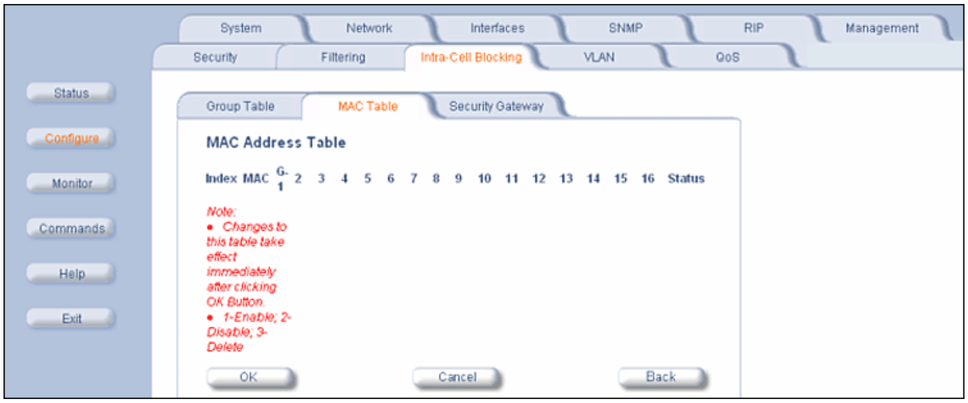
Note:

- *Additions to this table take effect immediately after clicking Add Button.*
- *Maximum 250 MACs can be added.*

Enter the MAC address of the SU. Select **Enable** from the drop-down menu for the Group Index

Click **Add**. The MAC address is assigned to the groups. Additions to the MAC Table take effect immediately after clicking the **Add** button.

You can **Enable**, **Disable**, **Delete**, or **Reassign** the groups for a MAC address by using the **Edit/Delete Table Entries** button. A maximum of 250 MAC addresses can be added among all filter groups.



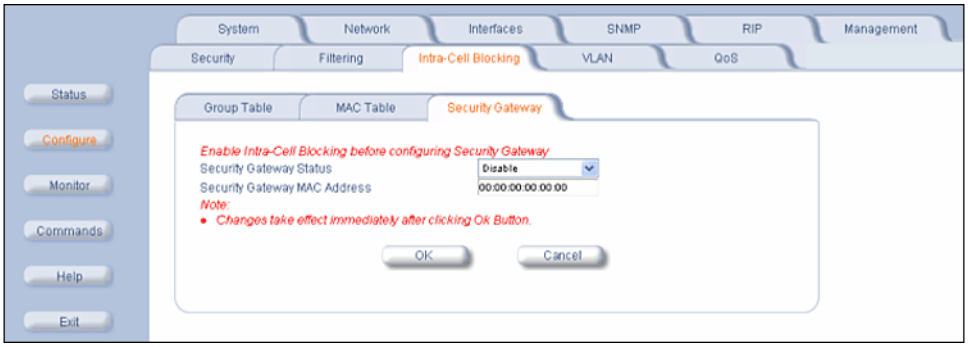
MAC Address Table

Index	MAC	G-1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Status

Note:
- *Changes to this table take effect immediately after clicking OK Button.*
- *1-Enable; 2-Disable; 3-Delete*

Block Traffic Between SUs (Security Gateway)

You can configure a Security Gateway to block traffic between SUs connected to different BSUs. Verify that Intra-Cell Blocking has been enabled on the **Group Table** tab before configuring the Security Gateway.



Enable Intra-Cell Blocking before configuring Security Gateway
Security Gateway Status: Disable
Security Gateway MAC Address: 00:00:00:00:00:00
Note:
- *Changes take effect immediately after clicking Ok Button.*

- **Security Gateway Status:** Enables or disables packet forwarding to the external Security Gateway.
- **Security Gateway MAC Address:** Lets you configure the MAC address of the external Security Gateway.

VLAN Parameters

Virtual LAN (VLAN) implementation in the Tsunami products:

- Lets the BSU and SU be used in a VLAN-aware network.
- Processes IEEE 802.1Q VLAN-tagged packets.

Network resources behind the BSU and SU can be assigned to logical groups.

Overview

VLAN Modes

Transparent Mode

Transparent mode is available on both the SU and the BSU. This mode is equivalent to NO VLAN support and is the default mode. It is used when the devices behind the SU and BSU are both VLAN aware and unaware. The SU/BSU transfers both tagged and untagged frames received on the Ethernet or WORP interface. Both tagged and untagged management frames can access the device.

Trunk Mode

Trunk mode VLAN is available on both the SU and the BSU. It is used when all devices behind the SU and BSU are VLAN aware. The SU and BSU transfer only tagged frames received on the Ethernet or WORP interface. Both tagged and untagged management frames can access the device.

Access Mode

Access mode is available only on the SU. It is used when the devices behind the SU are VLAN unaware. Frames to and from the Ethernet interface behind the SU map into only one VLAN segment.

Frames received on the Ethernet interface are tagged with the configured Access VLAN ID before forwarding them to the WORP interface. Both tagged and untagged management frames can access the device from the WORP interface. However, only untagged management frames can access the device from the Ethernet Interface.

VLAN Forwarding

The VLAN Trunk mode provides a means to configure a list of VLAN IDs in a Trunk VLAN Table. The SU and BSU only forward frames (between Ethernet and WORP interface) tagged with the VLAN IDs configured in the Trunk VLAN Table. Up to 256 VLAN IDs can be configured for the BSU and up to 16 VLAN IDs can be configured for the SU (depending upon the capabilities of your switching equipment).

VLAN Relaying

The VLAN Trunk mode for BSU operation provides an option to enable and disable a VLAN relaying flag; when enabled, the BSU shall relay frames between SUs on the same BSU having the same VLAN ID.

Management VLAN

The BSU and SU allow the configuration of a separate VLAN ID and priority for SNMP, ICMP, Telnet, and TFTP management frames for device access.

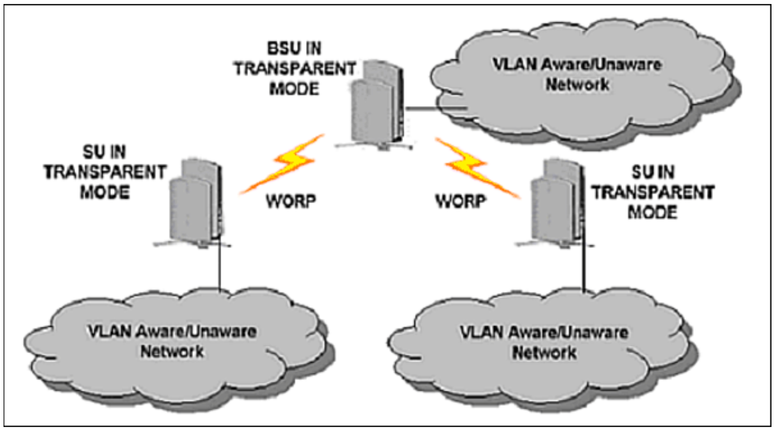
The management VLAN ID and management VLAN priority may be applied in any mode. The management stations tag the management frames they send to the BSU or SU with the management VLAN ID configured in the device. The BSU and SU tag all the management frames from the device with the configured management VLAN and priority.

BSU and SU in Transparent Mode

When the BSU is in Transparent mode, all associated SUs must be in Transparent mode.

How the BSU and SUs function in Transparent mode is described in the following table.

BSU Function – Transparent Mode	SU Function – Transparent Mode
• BSU forwards both tagged and untagged frames received from the Ethernet interface or from any of the associated SUs. • If a valid management VLAN ID is configured, BSU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, BSU tags all management frames generated by the BSU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), BSU allows only untagged management frames to access it.	• SU forwards both tagged and untagged frames received from the Ethernet interface or from the BSU. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access them.

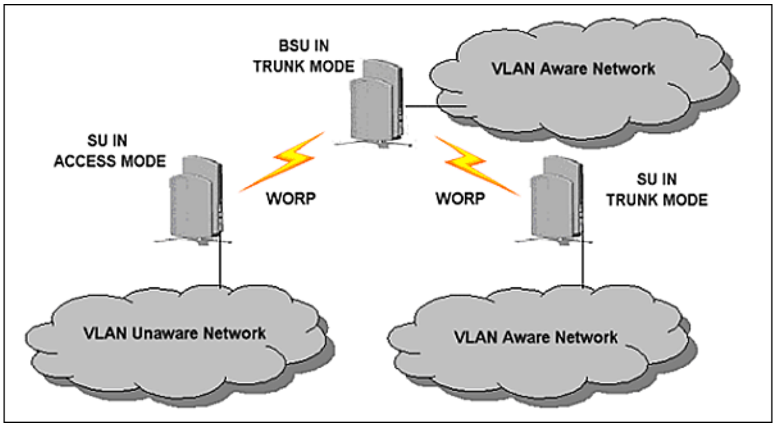

BSU IN TRANSPARENT MODE
VLAN Aware/Unaware Network
SU IN TRANSPARENT MODE
WORP
WORP
SU IN TRANSPARENT MODE
VLAN Aware/Unaware Network
VLAN Aware/Unaware Network

BSU in Trunk Mode and SU in Trunk/Access Mode

When the BSU is in Trunk mode, the associated SUs must be in either Trunk mode or Access mode. When an SU associates to a BSU that is in Trunk mode, it gets the VLAN mode from the BSU.

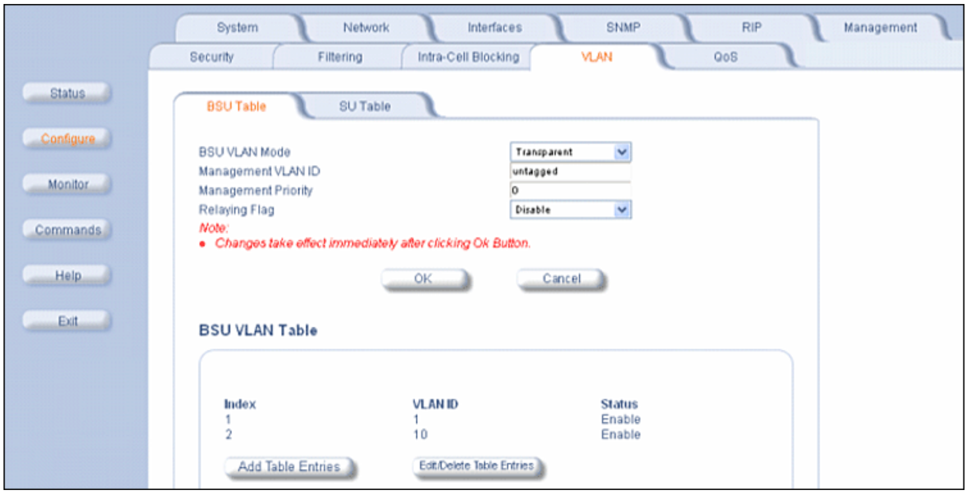
How the BSU and SU function in Trunk mode, and the SU in Access mode, is described in the following table.

BSU Function – Trunk Mode	SU Function – Trunk Mode	SU Function – Access Mode
• Up to 256 VLAN IDs can be configured on a BSU. • BSU discards all untagged frames received from the Ethernet interface or from any of the associated SUs (unexpected). • If a valid VLAN ID is configured, BSU forwards only VLAN-tagged frames received from the Ethernet interface or from any of the associated SUs that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, BSU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, BSU tags all management frames generated by the BSU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), BSU allows only untagged management frames to access it.	• Up to 16 VLAN IDs can be configured on an SU. • SU discards all untagged frames received from the Ethernet interface or from the BSU (unexpected). • If a valid VLAN ID is configured, SU forwards only VLAN-tagged frames received from the Ethernet interface or from the BSU that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it.	• SU discards all tagged frames received from the Ethernet interface and all untagged frames received from the BSU (unexpected). • SU tags all untagged frames received from the Ethernet interface with the configured Access VLAN ID and forwards them to the BSU. • SU untags all tagged frames received from the BSU that are tagged with the configured Access VLAN ID and forwards them to the Ethernet interface; it discards all other tagged frames from the BSU. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it from the BSU. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority and forwards them to the BSU. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it from the BSU. • SU allows only untagged management frames to access it from the Ethernet interface, regardless of the value of the management VLAN ID.



BSU VLAN Configuration

The HTTP Interface to configure BSU VLAN parameters is shown in the following figure.



BSU VLAN Mode	Transparent
Management VLAN ID	untagged
Management Priority	0
Relaying Flag	Disable

Note:
- *Changes take effect immediately after clicking Ok Button.*

BSU VLAN Table

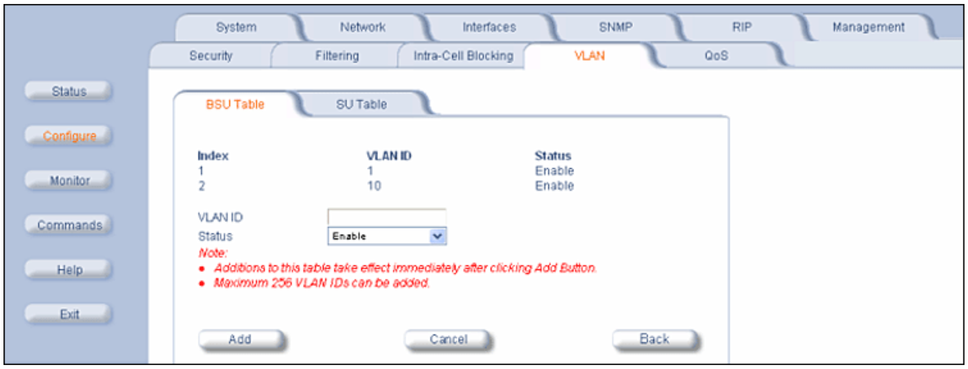
Index	VLAN ID	Status
1	1	Enable
2	10	Enable

The following parameters are configurable:

- **BSU VLAN Mode:** The BSU VLAN mode can be either Transparent or Trunk. By default, the BSU is in Transparent mode.
- **Management VLAN ID:** The Management VLAN ID is configurable in any mode. The management VLAN ID has a default value of untagged and may be configured with a value in the range of 1 to 4095.
- **Management VLAN Priority:** The Management VLAN priority values range from 0 to 7 and the default priority is 0 (zero).
- **Relaying Flag:** When this flag is enabled, the BSU relays frames between SUs on the same BSU.
- **BSU VLAN Table:** The BSU VLAN Table is configurable in both Transparent and Trunk mode, but applies only when the BSU is in Trunk mode. The VLAN ID values for the BSU VLAN Table range from 1 to 4095. The maximum number of VLAN IDs that can be configured in the BSU VLAN Table is 256. An SU in Trunk mode is assigned VLAN IDs from this table.

Add BSU VLAN Table Entries

To add entries to the BSU VLAN table, click the **Add Table Entries** button. Enter a **VLAN ID** and select a **Status**, then click **Add** to add your entry to the table.



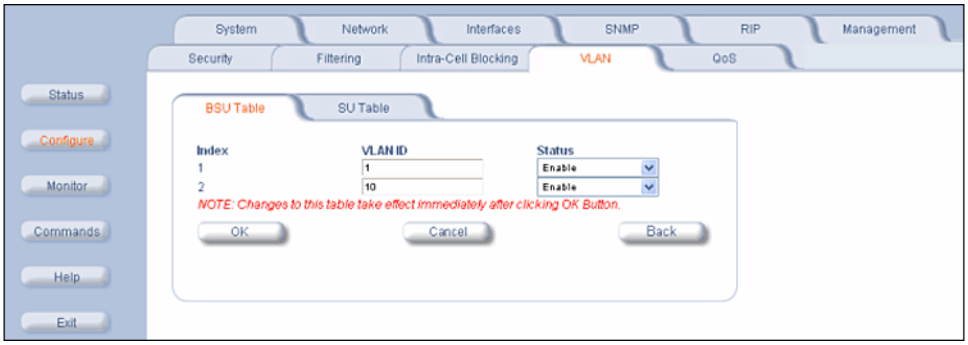
Index	VLAN ID	Status
1	1	Enable
2	10	Enable

VLAN ID	
Status	Enable

Note:
- *Additions to this table take effect immediately after clicking Add Button.*
- *Maximum 256 VLAN IDs can be added.*

Edit or Delete BSU VLAN Table Entries

To edit or delete entries in the BSU VLAN Table, click the **Edit/Delete Table Entries** button, make your changes, then click **OK** for your changes to take effect.



Index	VLAN ID	Status
1	1	Enable
2	10	Enable

NOTE: Changes to this table take effect immediately after clicking OK Button.

Restricting Unit Management

Management access to the unit can be easily secured by making management stations or hosts and the unit itself members of a common VLAN. Simply configure a non-zero management VLAN ID: management of the unit will be restricted to members of the same VLAN.

CAUTION: *If a non-zero management VLAN ID is configured, management access to the unit is restricted to hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the unit or you will lose access to the unit.*

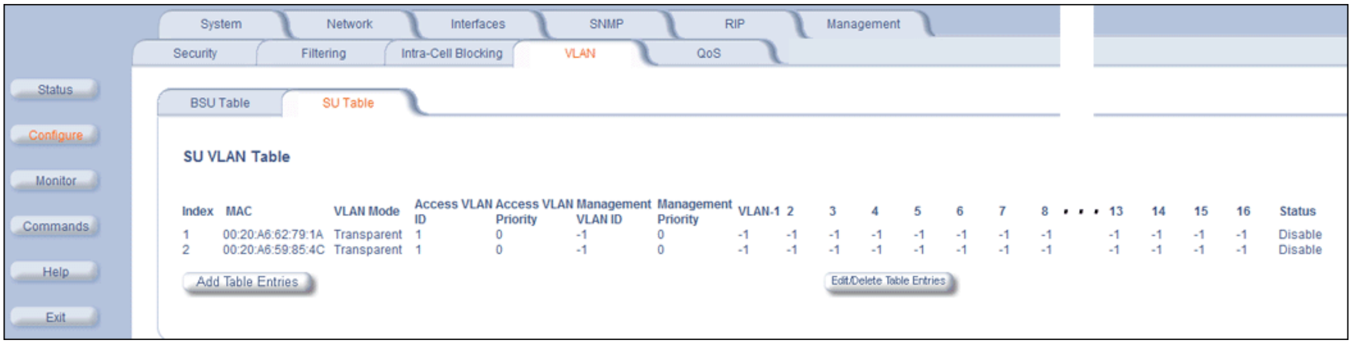
Providing Access to Hosts in the Same VLAN

The VLAN feature lets hosts manage the unit. If the **Management VLAN ID** matches a VLAN User ID, those hosts who are members of that VLAN will have management access to the unit.

CAUTION: *Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs, all members of that VLAN will have management access to the unit. Be careful to restrict VLAN membership to those with legitimate access to the unit.*

SU VLAN Configuration

The HTTP Interface to configure SU VLAN parameters is shown in the following figure.

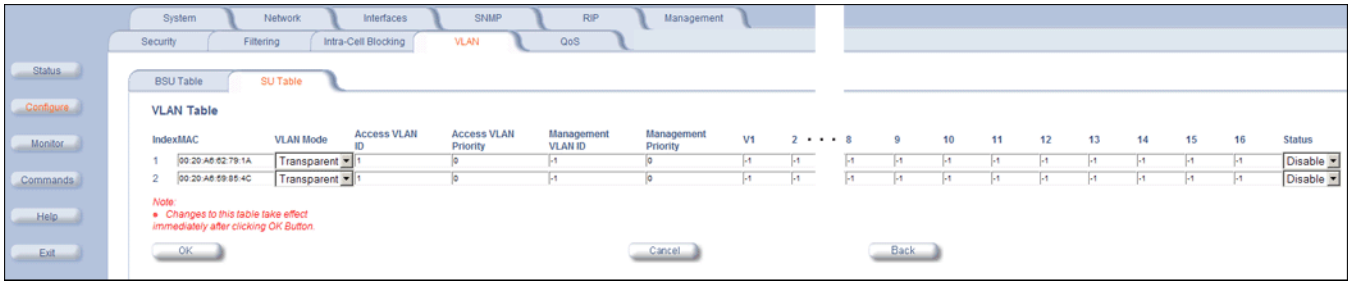


SU VLAN Table

Index	MAC	VLAN Mode	Access VLAN ID	Access VLAN Priority	Management VLAN ID	Management Priority	VLAN-1	2	3	4	5	6	7	8	• • •	13	14	15	16	Status
1	00:20:A6:62:79:1A	Transparent	1	0	-1	0	-1	-1	-1	-1	-1	-1	-1	-1		-1	-1	-1	-1	Disable
2	00:20:A6:59:85:4C	Transparent	1	0	-1	0	-1	-1	-1	-1	-1	-1	-1	-1		-1	-1	-1	-1	Disable

Add SU Table Entries

To add entries to the SU VLAN Table, click the **Add Table Entries** button. Enter the desired parameters in the corresponding fields, then click **Add** to add and save the entry.



VLAN Table

IndexMAC		VLAN Mode	Access VLAN ID	Access VLAN Priority	Management VLAN ID	Management Priority	V1	2 • • •	8	9	10	11	12	13	14	15	16	Status
1	00:20:A6:62:79:1A	Transparent	1	0	-1	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	Disable
2	00:20:A6:59:85:4C	Transparent	1	0	-1	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	Disable

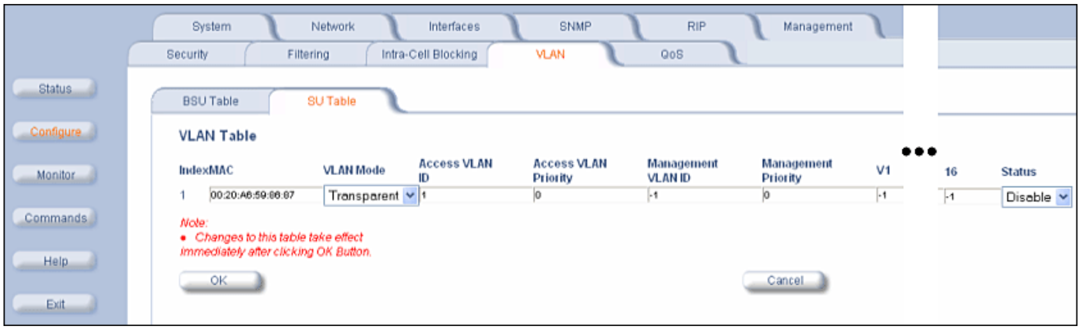
Note:
- *Changes to this table take effect immediately after clicking OK Button.*

The following parameters are configurable:

- **MAC:** Enter the MAC address of the SU to be configured.
- **SU VLAN Mode:** The SU VLAN mode can be either Transparent, Trunk, or Access (by default, the BSU is in Transparent mode).
  - When the BSU is in Transparent mode, the SU must be in Transparent mode.
  - When the BSU is in Trunk mode, the SU must be in either Access mode or Trunk mode.
  - When the BSU is changed from Transparent mode to Trunk mode, all the configured SUs are changed to Trunk mode by default.
- **Access VLAN ID:** The **A**ccess VLAN ID is configurable in any mode, but applies only when the SU is in Access mode. The Access VLAN ID values range from 1 to 4095; the default value is 1.
- **Access VLAN Priority:** The Access VLAN Priority is configurable in any mode, but applies only when the SU is in Access mode. The Access VLAN priority values range from 0 to 7; the default priority is 0. For voice frames, the priority field is set to the VoIP configured value (5 according to latest IETF draft, or 6 according to IEEE 802.1D) regardless of the priority value configured.
- **Management VLAN ID:** The management VLAN ID is configurable in any mode. The management VLAN ID has a default value of **untagged** (-1) and may be configured with a value in the range of 1 to 4095.
- **Management Priority:** The Management VLAN priority values range from 0 to 7 and the default priority is 0 (zero).
- **VLAN 1-16:** The VLAN IDs are configurable in any mode, but apply only when the SU is in Trunk mode. The VLAN ID values range from 1 to 4095; the default value is untagged (-1). The maximum number of VLAN IDs that can be configured in the SU VLAN Table is 16 for each SU. The SU VLAN IDs must be in the BSU VLAN Table that corresponds to the BSU.

Edit SU Table Entries

To edit SU table entries, click the **Edit/Delete Table Entries** button; make your changes on the window displayed, then click **OK** to save your changes.



VLAN Table

IndexMAC		VLAN Mode	Access VLAN ID	Access VLAN Priority	Management VLAN ID	Management Priority	V1	••• 16	Status
1	00:20:A6:59:86:87	Transparent	1	0	-1	0	-1	-1	Disable

Note:
- *Changes to this table take effect immediately after clicking OK Button.*

Typical User VLAN Configurations

VLANs segment network traffic into groups, which lets you limit broadcast and multicast traffic. These groups enable hosts from different VLANs to access different resources using the same network infrastructure. Hosts using the same physical network are limited to those resources available to their workgroup.

The unit can segment users into a maximum of 16 different VLANs per unit, based upon a VLAN ID.

The primary scenarios for using VLAN workgroups are as follows:

- **VLAN disabled:** Your network does not use VLANs.
- **VLAN enabled:** Each VLAN workgroup uses a different VLAN ID Tag. A mixture of Tagged and Untagged workgroups may be supported.

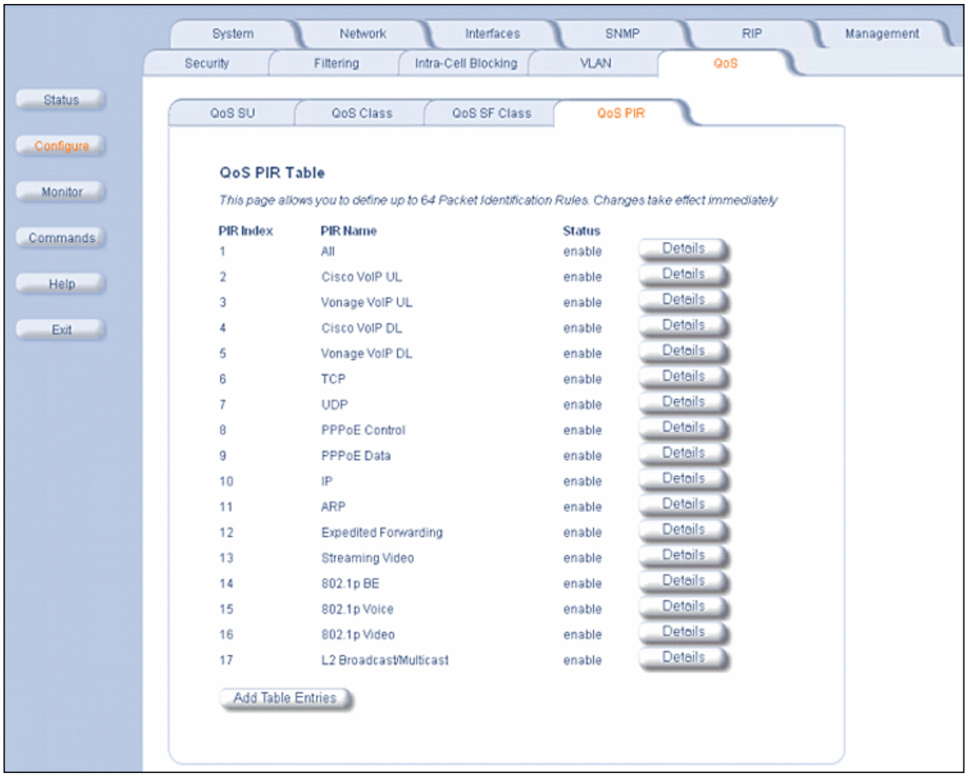
QoS (Quality of Service) Parameters

The Quality of Service (QoS) feature is based on 802.16 standard and defines the classes, service flows (SFCs), and packet identification rules (PIRs) for specific types of traffic. The main priority of QoS is to guarantee a reliable and adequate transmission quality for all traffic types under conditions of high congestion and bandwidth over-subscription (for a complete discussion on QoS see Quality of Service (QoS).

There are already several pre-defined QoS classes, SFCs and PIRs available that you may choose from which cover the most common types of traffic. If you want to configure something else, you start building the hierarchy of a QoS class by defining PIRs; then you associate some of those PIRs to specific Service Flow classes (SFCs); you assign priorities to each PIR within each SFC; and finally you define the QoS class by associating relevant SFCs to each QoS class.

QoS PIR Configuration

Click **Configure** > **QoS** > **QoS PIR Table**. The 17 predefined PIRs are shown.



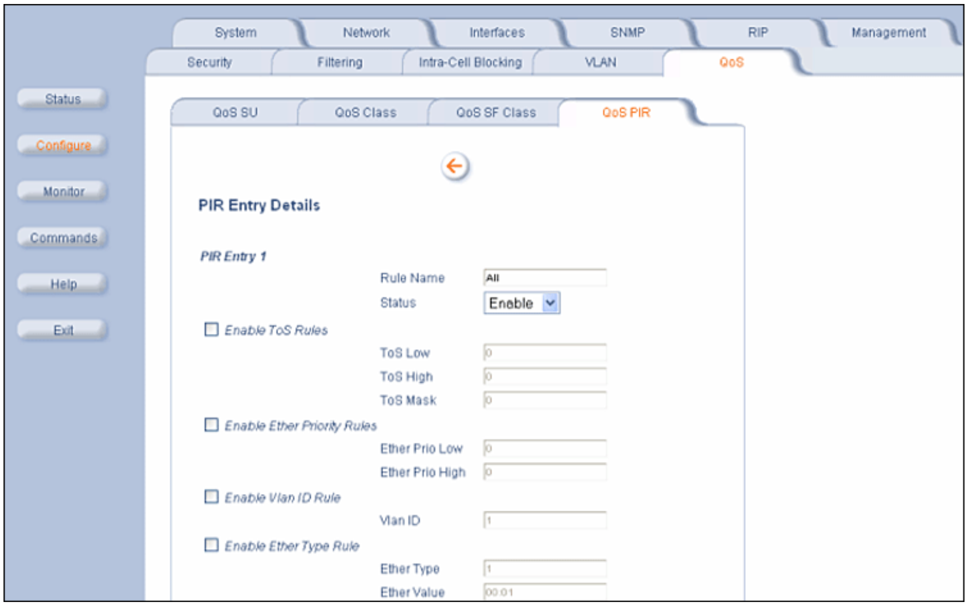
QoS PIR Table

This page allows you to define up to 64 Packet Identification Rules. Changes take effect immediately

PIR Index	PIR Name	Status	
1	All	enable	Details
2	Cisco VoIP UL	enable	Details
3	Vonage VoIP UL	enable	Details
4	Cisco VoIP DL	enable	Details
5	Vonage VoIP DL	enable	Details
6	TCP	enable	Details
7	UDP	enable	Details
8	PPPoE Control	enable	Details
9	PPPoE Data	enable	Details
10	IP	enable	Details
11	ARP	enable	Details
12	Expedited Forwarding	enable	Details
13	Streaming Video	enable	Details
14	802.1p BE	enable	Details
15	802.1p Voice	enable	Details
16	802.1p Video	enable	Details
17	L2 Broadcast/Multicast	enable	Details

Add Table Entries

To view/edit the parameters of each PIR click on its **Details** button. You may enable, disable or delete any PIR entry by clicking on the **Status** drop-down box and then clicking **OK**.



PIR Entry Details

PIR Entry 1

Rule Name: All
Status: Enable

☐ *Enable ToS Rules*

ToS Low: 0
ToS High: 0
ToS Mask: 0

☐ *Enable Ether Priority Rules*

Ether Prio Low: 0
Ether Prio High: 0

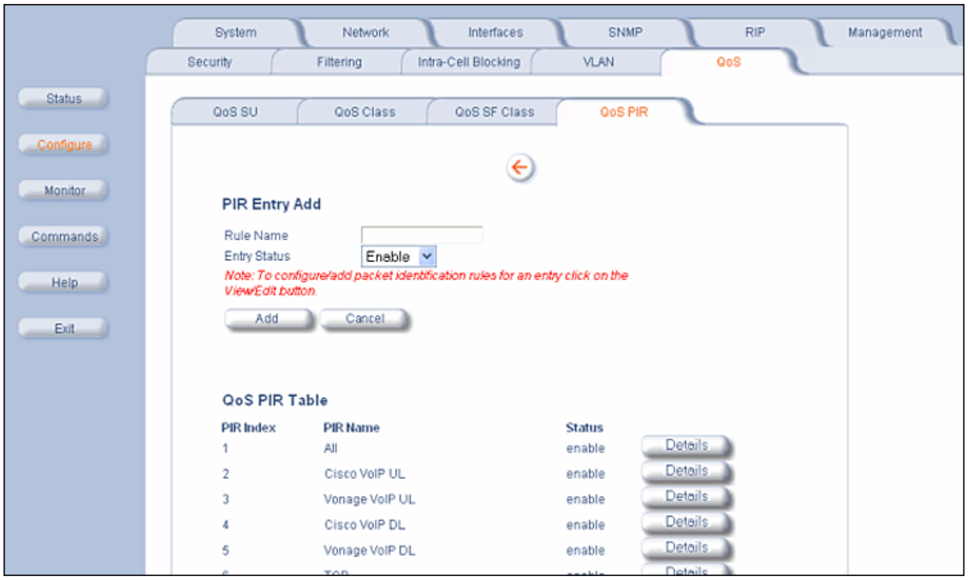
☐ *Enable Vlan ID Rule*

Vlan ID: 1

☐ *Enable Ether Type Rule*

Ether Type: 1
Ether Value: 00:01

To add entries to the PIR Table, click the **Add Table Entries** button. Enter the **Rule Name** and select Enable or Disable from the **Entry Status** drop-down box, then click **Add** to add the entry. Once the new entry appears on the screen (as shown below), click its **Details** button to view/edit its parameters.



PIR Entry Add

Rule Name:
Entry Status: Enable

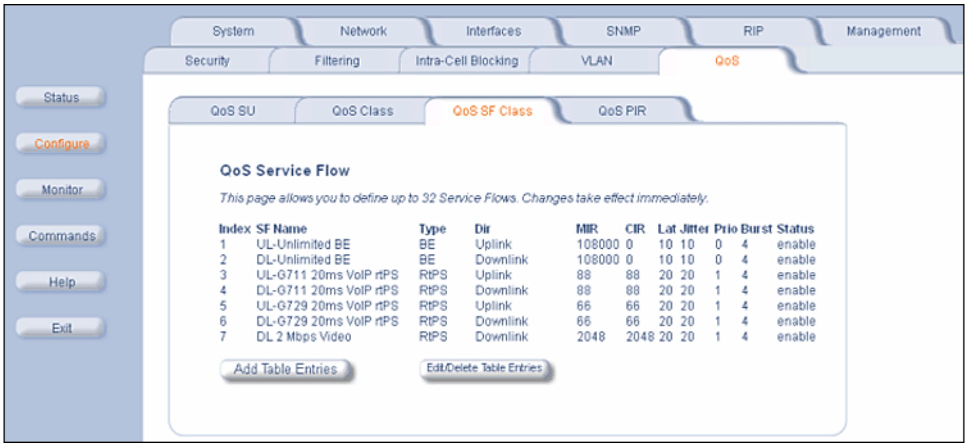
Note: To configure/add packet identification rules for an entry click on the View/Edit button.

QoS PIR Table

PIR Index	PIR Name	Status	
1	All	enable	Details
2	Cisco VoIP UL	enable	Details
3	Vonage VoIP UL	enable	Details
4	Cisco VoIP DL	enable	Details
5	Vonage VoIP DL	enable	Details
6	TCP	enable	Details

QoS SFC Configuration

Click **Configure** > **QoS** > **QoS SF Class**. The 7 predefined SFCs are shown.

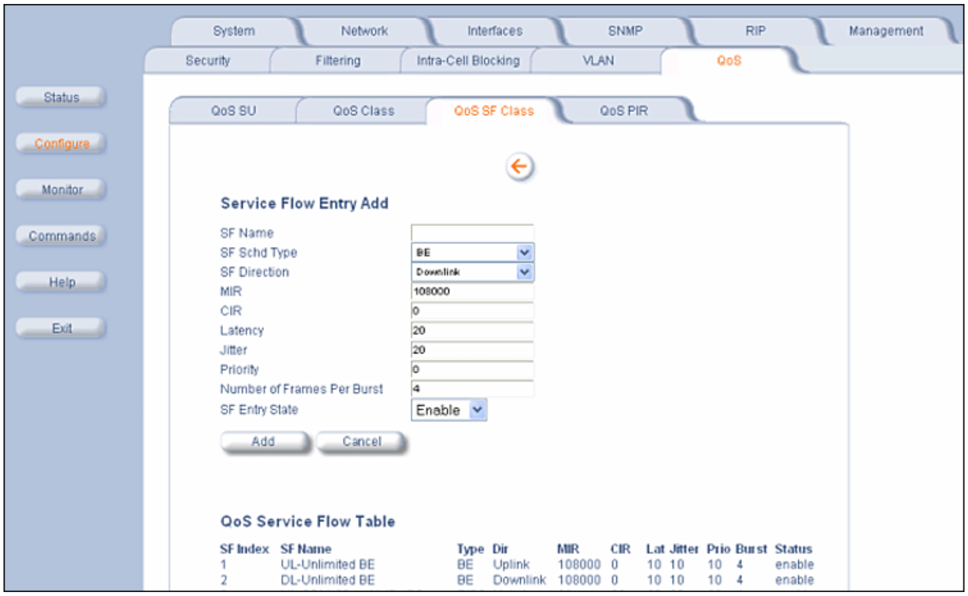


QoS Service Flow

This page allows you to define up to 32 Service Flows. Changes take effect immediately.

Index	SF Name	Type	Dir	MIR	CIR	Lat	Jitter	Prio	Burst	Status
1	UL-Unlimited BE	BE	Uplink	108000	0	10	10	0	4	enable
2	DL-Unlimited BE	BE	Downlink	108000	0	10	10	0	4	enable
3	UL-G711 20ms VoIP rtPS	RtPS	Uplink	88	88	20	20	1	4	enable
4	DL-G711 20ms VoIP rtPS	RtPS	Downlink	88	88	20	20	1	4	enable
5	UL-G729 20ms VoIP rtPS	RtPS	Uplink	66	66	20	20	1	4	enable
6	DL-G729 20ms VoIP rtPS	RtPS	Downlink	66	66	20	20	1	4	enable
7	DL 2 Mbps Video	RtPS	Downlink	2048	2048	20	20	1	4	enable

To add entries to the SFC Table, click the **Add Table Entries** button.



Service Flow Entry Add

SF Name	
SF Schd Type	BE
SF Direction	Downlink
MIR	108000
CIR	0
Latency	20
Jitter	20
Priority	0
Number of Frames Per Burst	4
SF Entry State	Enable

QoS Service Flow Table

SF Index	SF Name	Type	Dir	MIR	CIR	Lat	Jitter	Prio	Burst	Status
1	UL-Unlimited BE	BE	Uplink	108000	0	10	10	10	4	enable
2	DL-Unlimited BE	BE	Downlink	108000	0	10	10	10	4	enable

The following parameters are configurable:

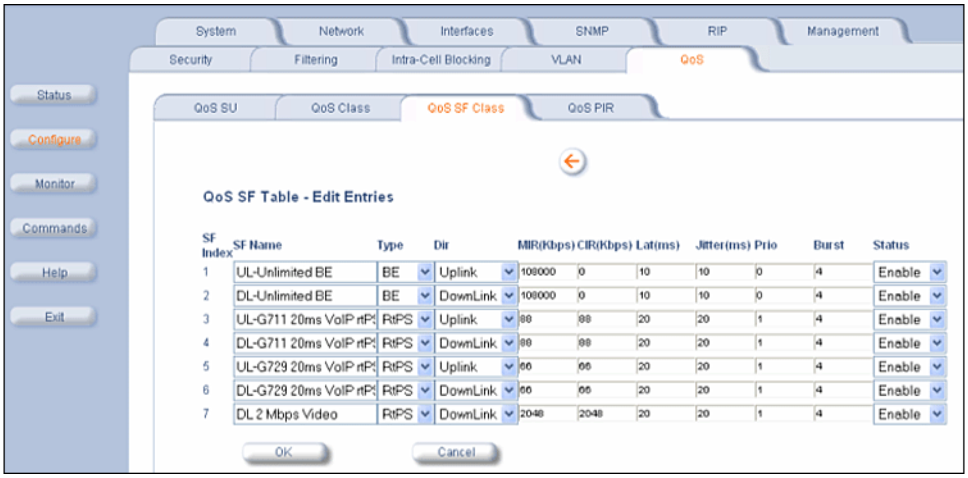
- **SF Name:** Enter the name of the SF class you want to add.
- **SF Schd Type:** This field can be set to BE (Best Effort) or RtPS (Real-Time Polling Service).
- **SF Direction:** This field can be set to Downlink (traffic from BSU to SU) or **Uplink** (traffic from SU to BSU).
- **MIR (Maximum Information Rate):** The maximum sustained data rate specified in units of 1 Kbps from 8 Kbps up to the maximum rate of 108000 Kbps per SU.
- **CIR (Committed Information Rate):** The minimum reserved traffic rate specified in units of 1 Kbps from 0 Kbps up to the maximum rate of 10000 Kbps per SU.
- **Latency:** The maximum allowed latency specified in increments of 5 ms steps from a minimum of 5 ms up to a maximum of 100 ms.
- **Jitter:** The maximum tolerable jitter specified in increments of 5 ms steps from a minimum of 0 ms up to the Maximum Latency (in ms).
- **Priority:** The priority of this SFC from zero (0) to seven (7), 0 being the lowest, 7 being the highest.
- **Number of Frames per Burst:** The Maximum number of data messages in a Multi-Frame burst from one (1) to four (4), which affects the percentage of the maximum throughput of the system according to following table.

No. of messages in a burst:	% of the maximum throughput:
4	100 %
3	97.6 %
2	92.9 %
1	76.2%

- **SF Entry State:** This field can be set to **Enable**, **Disable**, or **Delete**.

Click **Add** to add the entry. The new entry will appear on the screen, taking up the next sequential index entry.

To make changes to the entries of the SFC Table, click the **Edit/Delete Table Entries** button.



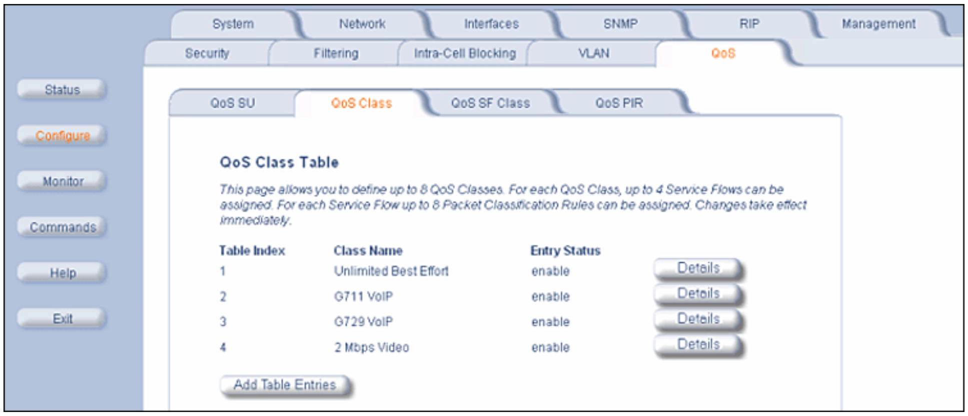
QoS SF Table - Edit Entries

SF Index	SF Name	Type	Dir	MIR(Kbps)	CIR(Kbps)	Lat(ms)	Jitter(ms)	Prio	Burst	Status
1	UL-Unlimited BE	BE	Uplink	108000	0	10	10	0	4	Enable
2	DL-Unlimited BE	BE	DownLink	108000	0	10	10	0	4	Enable
3	UL-G711 20ms VoIP rtP:	RtPS	Uplink	88	88	20	20	1	4	Enable
4	DL-G711 20ms VoIP rtP:	RtPS	DownLink	88	88	20	20	1	4	Enable
5	UL-G729 20ms VoIP rtP:	RtPS	Uplink	66	66	20	20	1	4	Enable
6	DL-G729 20ms VoIP rtP:	RtPS	DownLink	66	66	20	20	1	4	Enable
7	DL 2 Mbps Video	RtPS	DownLink	2048	2048	20	20	1	4	Enable

Enter your changes and click **OK**. To delete an entry, click the **Status** drop-down box and select **Delete**, then click **OK**.

QoS Class Configuration

Click **Configure** > **QoS** > **QoS Class**. The 4 predefined QoS classes are shown.

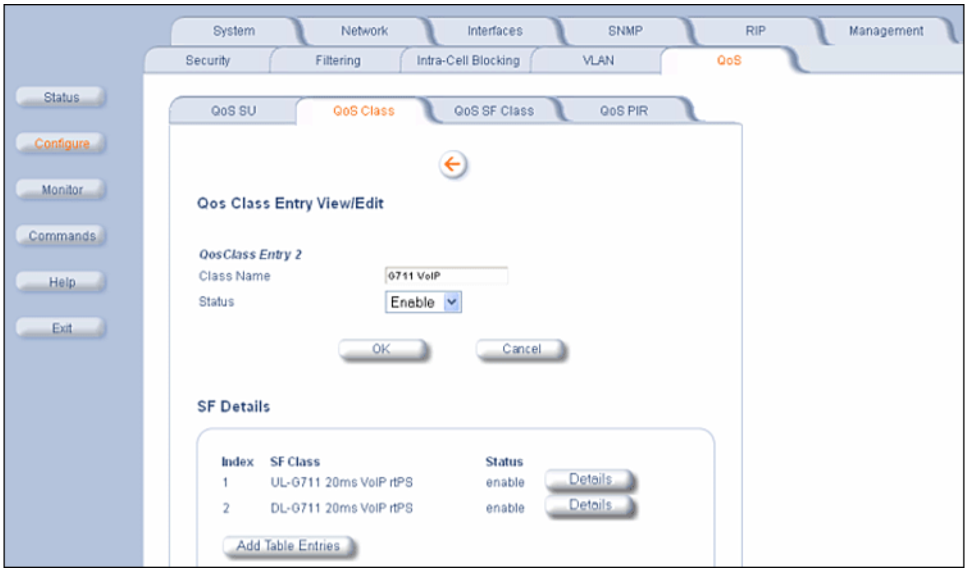


QoS Class Table

This page allows you to define up to 8 QoS Classes. For each QoS Class, up to 4 Service Flows can be assigned. For each Service Flow up to 8 Packet Classification Rules can be assigned. Changes take effect immediately.

Table Index	Class Name	Entry Status	
1	Unlimited Best Effort	enable	Details
2	G711 VoIP	enable	Details
3	G729 VoIP	enable	Details
4	2 Mbps Video	enable	Details

To view/edit a QoS Class click on its **Details** button. You may enable, disable or delete this QoS Class entry by clicking on the **Status** drop-down box and then clicking **OK**. You may also edit an existing SFC associated to this QoS class, or add a new SFC.



Qos Class Entry View/Edit

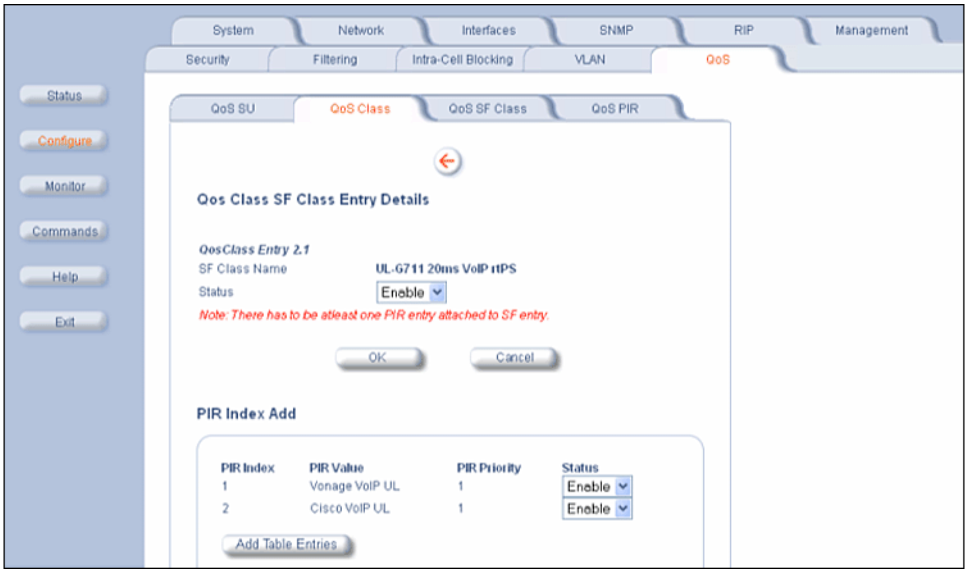
QosClass Entry 2

Class Name	G711 VoIP
Status	Enable

SF Details

Index	SF Class	Status
1	UL-G711 20ms VoIP rtPS	enable
2	DL-G711 20ms VoIP rtPS	enable

To edit an existing SFC associated to this QoS Class click its **Details** button. You may enable, disable or delete this SFC entry by clicking on the **Status** drop-down box and then clicking **OK**. You may also delete a PIR associated to this SFC by clicking on the **Status** drop-down box and then clicking **OK**, or add a new PIR to this SFC.



Qos Class SF Class Entry Details

QosClass Entry 2.1

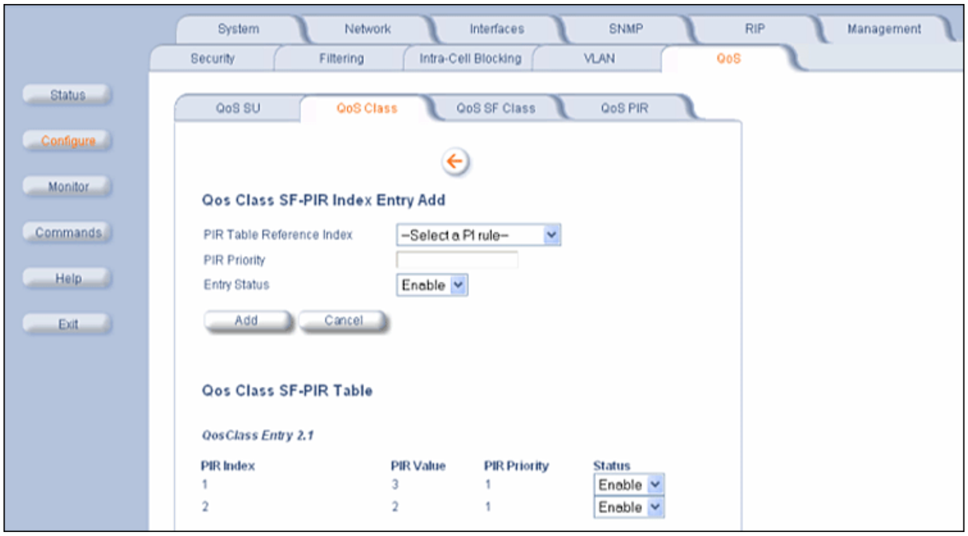
SF Class Name	UL-G711 20ms VoIP rtPS
Status	Enable

Note: There has to be atleast one PIR entry attached to SF entry.

PIR Index Add

PIR Index	PIR Value	PIR Priority	Status
1	Vonage VoIP UL	1	Enable
2	Cisco VoIP UL	1	Enable

To add more PIRs to this SFC click the **Add Table Entries** button.



Qos Class SF-PIR Index Entry Add

PIR Table Reference Index	–Select a PI rule–
PIR Priority	
Entry Status	Enable

Qos Class SF-PIR Table

QosClass Entry 2.1

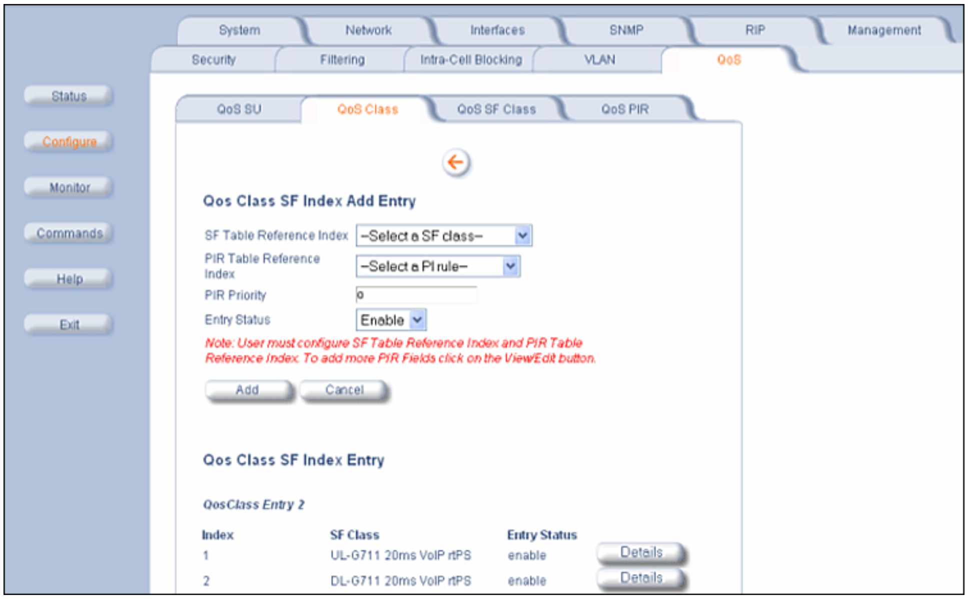
PIR Index	PIR Value	PIR Priority	Status
1	3	1	Enable
2	2	1	Enable

The following parameters are configurable:

- **PIR Table Reference Index:** Select one of the possible PIRs that have been previously configured from the drop-down box.
- **PIR Priority:** This priority per rule defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
- **Entry Status:** This field is always set to **Enable**.

Click **Add** to add the entry. The new entry will show up on the screen taking up the next sequential index entry. You may delete any PIR entry by clicking on the **Status** drop-down box.

Back on the QoS Class screen, click the **Add Table Entries** button to add a new SFC and associate it to this QoS Class.



Qos Class SF Index Add Entry

SF Table Reference Index	–Select a SF class–
PIR Table Reference Index	–Select a PI rule–
PIR Priority	0
Entry Status	Enable

Note: User must configure SF Table Reference Index and PIR Table Reference Index. To add more PIR Fields click on the View/Edit button.

Qos Class SF Index Entry

QosClass Entry 2

Index	SF Class	Entry Status	
1	UL-G711 20ms VoIP rtPS	enable	Details
2	DL-G711 20ms VoIP rtPS	enable	Details

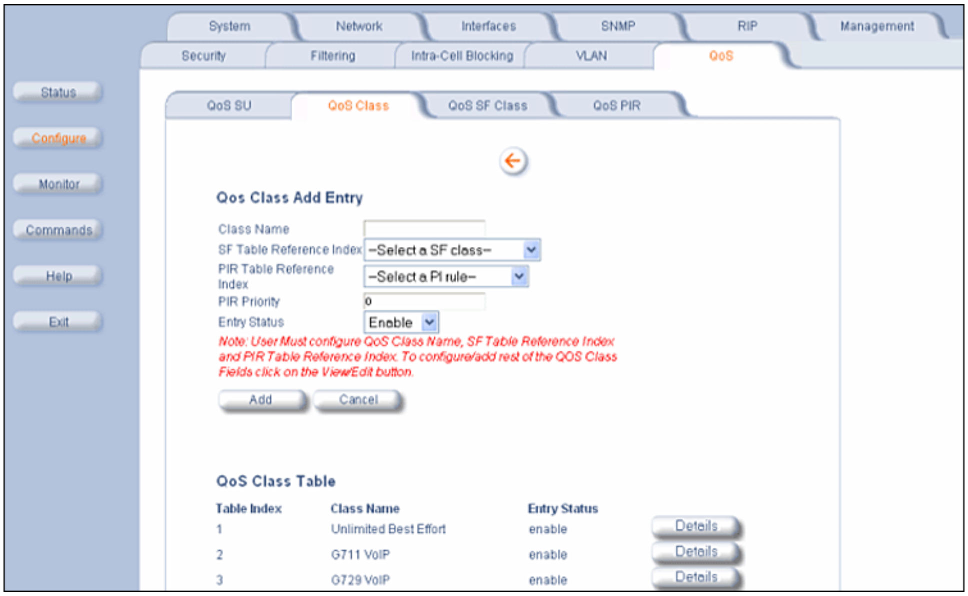
The following parameters are configurable:

- **SF Table Reference Index:** Select one of the possible SFCs that have been previously configured from the drop-down box to associate to this QoS Class.
- **PIR Table Reference Index:** Select one of the possible PIRs that have been previously configured from the drop-down box to associate to this SFC.
- **PIR Priority:** This priority per rule defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
- **Entry Status:** This field is always set to **Enable**.

Click Add to add the entry. The new entry will show up on the screen taking up the next sequential index entry.

From this screen you may also edit an existing SFC by clicking on its **Details** button. This will take you back to the QoS Class SF Class Entry Details.

Finally, to add a new QoS Class click the **Add Table Entries** button on the screen.



Qos Class Add Entry

Class Name	
SF Table Reference Index	–Select a SF class–
PIR Table Reference Index	–Select a PI rule–
PIR Priority	0
Entry Status	Enable

Note: User Must configure QoS Class Name, SF Table Reference Index and PIR Table Reference Index. To configure/add rest of the QOS Class Fields click on the View/Edit button.

QoS Class Table

Table Index	Class Name	Entry Status	
1	Unlimited Best Effort	enable	Details
2	G711 VoIP	enable	Details
3	G729 VoIP	enable	Details

The following parameters are configurable:

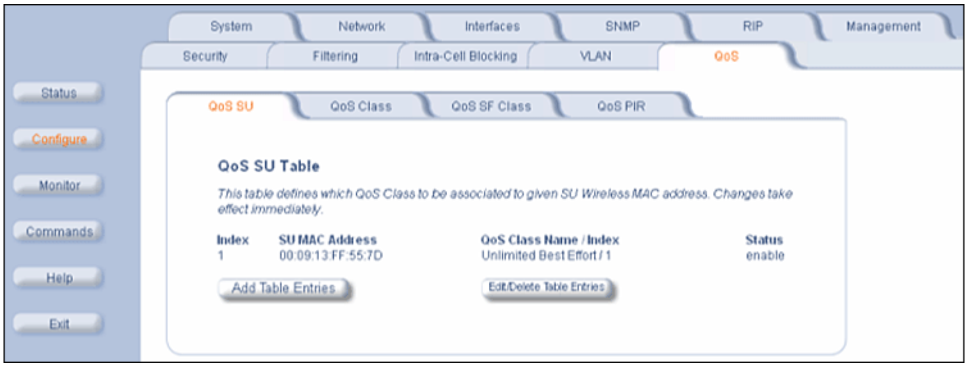
- **Class Name:** Enter the name of the QoS class you want to add.
- **SF Table Reference Index:** Select one of the possible SFCs that have been previously configured from the drop-down box to associate to this QoS Class.
- **PIR Table Reference Index:** Select one of the possible PIRs that have been previously configured from the drop-down box to associate to this SFC.
- **PIR Priority:** This priority per rule defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
- **Entry Status:** This field is always set to **Enable**.

Click **Add** to add the entry. The new entry will show up on the screen taking up the next sequential index entry.

From this screen you may also edit an existing QoS Class by clicking on its **Details** button. This will take you to the QoS Class Entry View/Edit screen.

QoS SU Configuration

Click **Configure** > **QoS** > **QoS SU**.



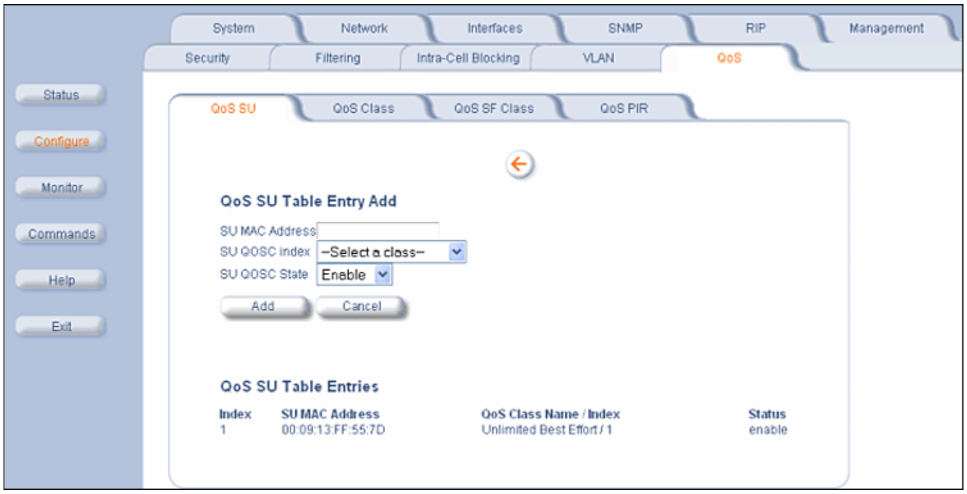
QoS SU Table

This table defines which QoS Class to be associated to given SU Wireless MAC address. Changes take effect immediately.

Index	SU MAC Address	QoS Class Name / Index	Status
1	00:09:13:FF:55:7D	Unlimited Best Effort / 1	enable

This screen defines which QoS Classes will be associated to which given SUs by using their MAC addresses.

To add entries to the QoS SU Table, click the **Add Table Entries** button.



QoS SU Table Entry Add

SU MAC Address
SU QOSC Index --Select a class--
SU QOSC State Enable

QoS SU Table Entries

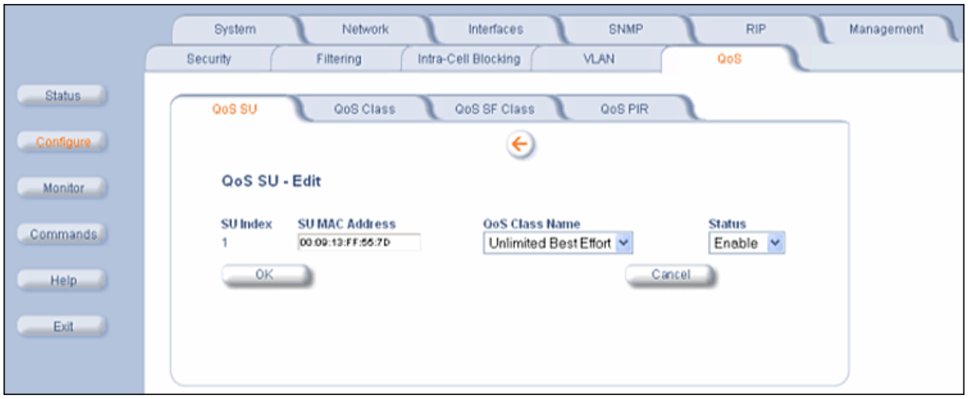
Index	SU MAC Address	QoS Class Name / Index	Status
1	00:09:13:FF:55:7D	Unlimited Best Effort / 1	enable

The following parameters are configurable:

- **SU MAC Address:** The MAC Address of the SU you want to associate to a specific QoS Class.
- **SU QOSC Index:** Select one of the possible QoS Classes that have been previously configured from the drop-down box to associate to this SU.
- **SU QOSC State:** This field can be set to **Enable**, **Disable**, or **Delete**.

Click **Add** to add the entry. The new entry will show up on the screen taking up the next sequential index entry.

To make changes to QoS SU Table, click the **Edit/Delete Table Entries** button.



QoS SU - Edit

SU Index	SU MAC Address	QoS Class Name	Status
1	00:09:13:FF:56:7D	Unlimited Best Effort	Enable

Enter your changes and click **OK**. To delete an entry, click the **Status** drop-down box and select **Delete**, then click **OK**.

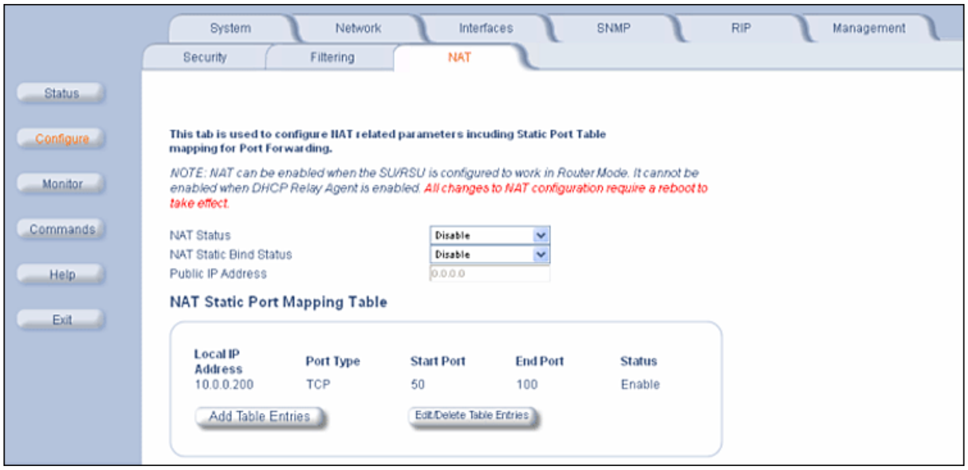
SU Access to the Public Network (NAT)

The NAT (Network Address Translation) feature lets hosts on the Ethernet side of the SU transparently access the public network through the BSU. All hosts in the private network can have simultaneous access to the public network.

NOTE: *The NAT tab is available for SUs in Routing mode only. The SU supports NAPT (Network Address Port Translation) where all private IP addresses are mapped to a single public IP address, and does not support Basic NAT (where private IP addresses are mapped to a pool of public IP addresses).*

Both ***dynamic mapping*** (allowing private hosts to access hosts in the public network) and ***static mapping*** (allowing public hosts to access hosts in the private network) are supported:

- In dynamic mapping, the SU maps the private IP addresses and its transport identifiers to transport identifiers of a single Public IP address as they originate sessions to the public network. This is used only for outbound access.
- Static mapping is used to provide inbound access. The SU maps a private IP address and its local port to a fixed public port of the global IP address. This is used to provide inbound access to a local server for hosts in the public network. Static port mapping allows only one server of a particular type. Up to 1000 ports (500 UDP and 500 TCP) are supported.



This tab is used to configure NAT related parameters incuding Static Port Table mapping for Port Forwarding.

NOTE: NAT can be enabled when the SU/RSU is configured to work in Router Mode. It cannot be enabled when DHCP Relay Agent is enabled. All changes to NAT configuration require a reboot to take effect.

NAT Status	Disable
NAT Static Bind Status	Disable
Public IP Address	0.0.0.0

NAT Static Port Mapping Table

Local IP Address	Port Type	Start Port	End Port	Status
10.0.0.200	TCP	50	100	Enable

The following parameters are configurable:

NOTE: *Changes to NAT parameters, including the NAT Static Port Mapping Table, require a reboot to take effect.*

NOTE: *When NAT is enabled, the DHCP Relay Agent feature is not supported (DHCP Relay Agent must be disabled before NAT is enabled) and RIP updates are not sent or received. You can configure a DHCP server to allocate IP addresses to hosts on the Ethernet side of the SU/ BSU (see* Enable and Configure the DHCP Server*).*

- **NAT Status:** Enables or disables the NAT feature. NAT can be enabled only for SUs in Routing mode. The default is disabled.
- **NAT Static Bind Status:** Enables or disables the NAT Static Bind status (static mapping) allowing public hosts to access hosts in a private network. The default is disabled.
- **Public IP Address:** The NAT Public IP address is the wireless interface IP address.

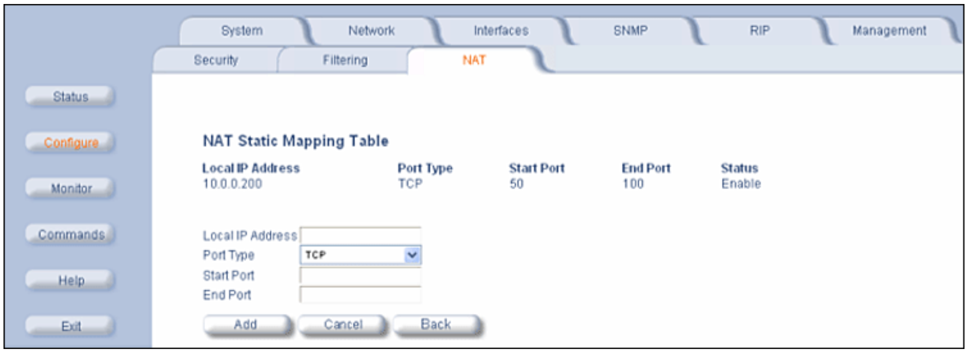
NAT Static Port Mapping Table

Adding entries to the NAT Static Mapping Table lets configured hosts in a private address realm on the Ethernet side of the SU access hosts in the public network using Network Address Port Translation (NAPT). Up to 1000 entries can be configured (500 UDP ports and 500 TCP ports).

Adding Entries

To add an entry:

1. Click the **Add Table Entries** button.
2. Enter the **Local IP Address** of the host on the Ethernet side of the SU.
3. Select the **Port Type**: **TCP**, **UDP**, or **Both**.
4. Enter the **Start Port** and **End Port**.
5. Click **Add**.



NAT Static Mapping Table

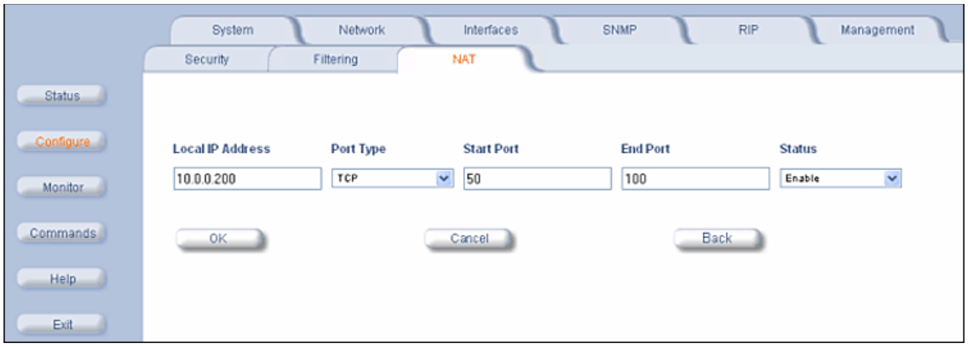
Local IP Address	Port Type	Start Port	End Port	Status
10.0.0.200	TCP	50	100	Enable

Local IP Address
Port Type TCP
Start Port
End Port

Editing Entries

To make changes to an entry:

1. Click the **Edit/Delete Table Entries** button.
2. Enter your changes. To delete an entry, click the **Status** drop-down box and select **Delete**
3. Click **OK**.



Local IP Address	Port Type	Start Port	End Port	Status
10.0.0.200	TCP	50	100	Enable

Supported Session Protocols

The NAT feature supports the following session protocols for both inbound and outbound access with the required support, applications, and limitations given in the following table.

Certain Internet applications require an Application Level Gateway (ALG) to provide the required transparency for an application running on a host in a private network to connect to its counterpart running on a host in the public network. An ALG may interact with NAT to set up state information, use NAT state information, modify application specific payload and perform the tasks necessary to get the application running across address realms.

No more than one server of a particular type is supported within the private network behind the SU.

These VPN protocols are supported with their corresponding ALGs: IPsec, PPTP, L2TP.

Supported Session Protocols			
Protocol	**Support**	**Applications**	**Limitations**
ICMP	ICMP ALG	Ping	

Supported Session Protocols			
Protocol	**Support**	**Applications**	**Limitations**
FTP	FTP ALG	File transfer	
H.323	H.323 ALG	Multimedia conferencing	
HTTP	Port mapping for inbound connection.	Web browser	
TFTP	Port mapping for inbound connection.	File transfer	
Telnet	Port mapping for inbound connection.	Remote login	
CUSeeMe	Port mapping for inbound and outbound connection.	Video conferencing	One user is allowed for video conferencing
IMAP	Port mapping for inbound connection.	Mail	
PNM	Port mapping for inbound connection.	Streaming media with Real Player	
POP3	Port mapping for inbound connection.	E-mail	
SMTP	Port mapping for inbound connection.	E-mail	Mails with IP addresses of MTAs or using IP addresses in place of FQDN are not supported (requires SMTP ALG).
RTSP	Port mapping for inbound connection.	Streaming audio/video with Quick Time and Real Player	
ICQ	Port mapping for inbound connection.	Chat and file transfer	Each host using ICQ needs to be mapped for different ports.
IRC	Port mapping for inbound connection.	Chat and file transfer	Each host using IRC needs to be mapped for different ports.
MSN Messenger	Port mapping for inbound and outbound connection.	Conference and Share files with Net meeting	Only one user is allowed for net meeting.
Net2Phone	Port mapping for inbound and outbound connection.	Voice communication	
IP Multicast	Pass Through	Multicasting	
Stream works	Port mapping for inbound connection.	Streaming video	
Quake	Port mapping for inbound connection.	Games	When a Quake server is configured within the private network behind a SU, the SU cannot provide information about that server on the public network. Also, certain Quake servers do not let multiple users log in using the same IP address, in which case only one Quake user is allowed.

Monitoring 7

This chapter describes using the Web interface to obtain detailed information about the settings and performance of the unit.

Click the **Monitor** button to access this information.

The following tabs appear in the **Monitor** section:

- Wireless (see Monitor the Wireless Settings)
- ICMP (see View Number of ICMP Messages)
- Per Station (see View Per Station Statistics)
- Features (see View Features Supported)
- Link Test (see Test Link Quality)
- Interfaces (see Monitor Interfaces)
- IP ARP Table (see View the Mapping of IP and MAC Addresses)
- IP Routes (see View Active IP Routes)
- Learn Table (see View All Detected MAC Addresses (Learn Table))
- RIP (see View RIP Data)
- Radius (see View RADIUS Traffic Information)
- QoS (see View Quality of Service (QoS) Information)
- Temperature (see View Temperature Log)

NOTE: *The* ***Radius*** *tab is available on BSUs only. The* ***RIP*** *tab is relevant only in Routing mode.*

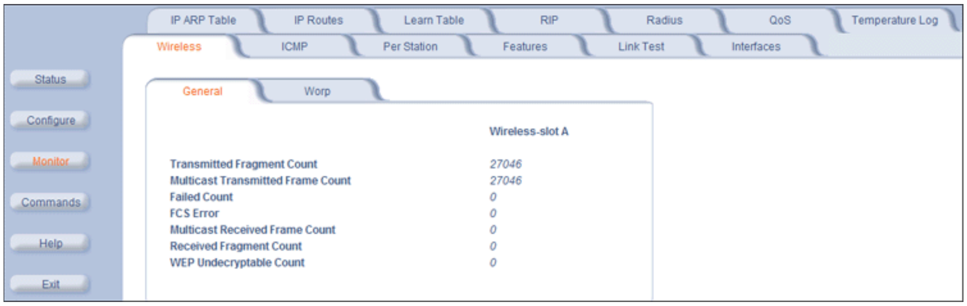
Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

Monitor the Wireless Settings

General Performance

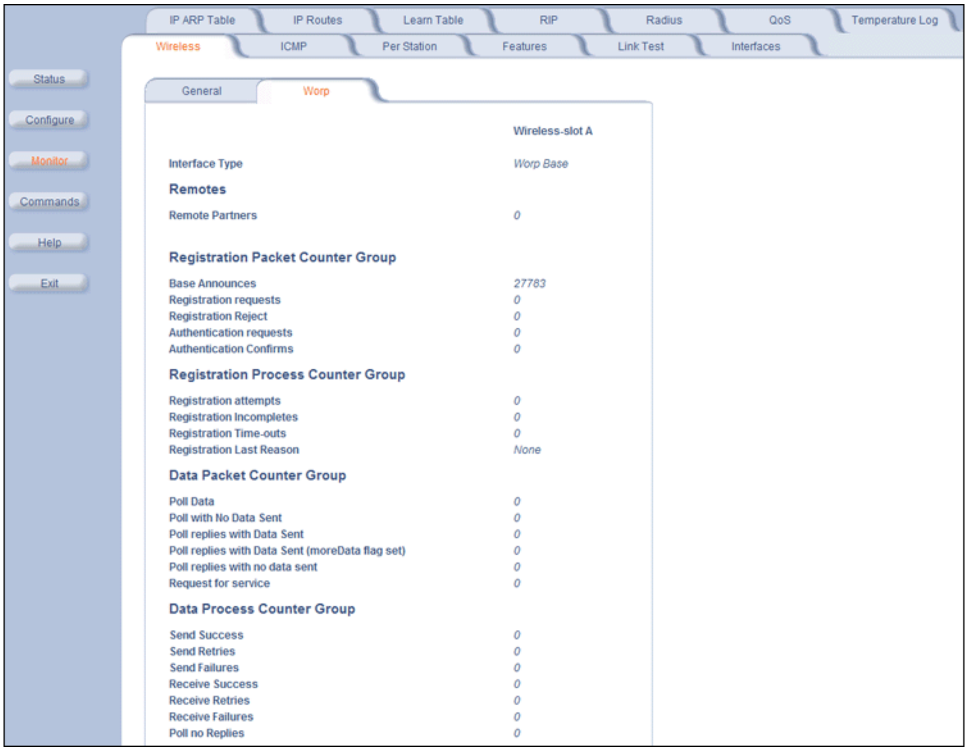
Click **Monitor** > **Wireless** > **General** to monitor the general performance of the wireless interface.



	Wireless-slot A
Transmitted Fragment Count	27046
Multicast Transmitted Frame Count	27046
Failed Count	0
FCS Error	0
Multicast Received Frame Count	0
Received Fragment Count	0
WEP Undecryptable Count	0

WORP Interface Performance

Click **Monitor** > **Wireless** > **WORP** tab to monitor the performance of the WORP Base or WORP SU interfaces.



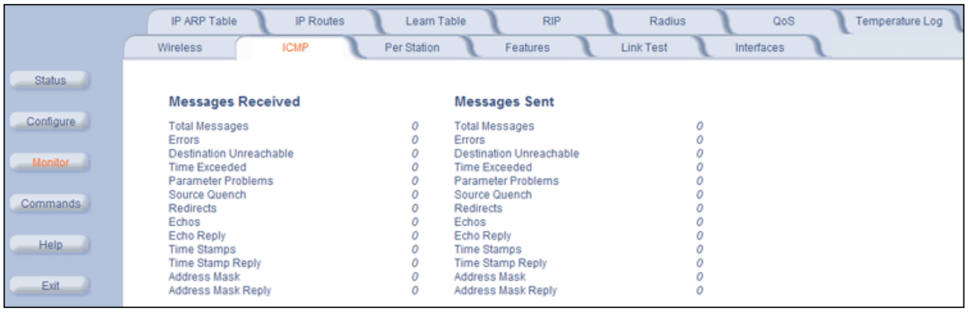
	Wireless-slot A
Interface Type	Worp Base
Remotes	
Remote Partners	0
Registration Packet Counter Group	
Base Announces	27783
Registration requests	0
Registration Reject	0
Authentication requests	0
Authentication Confirms	0
Registration Process Counter Group	
Registration attempts	0
Registration Incompletes	0
Registration Time-outs	0
Registration Last Reason	None
Data Packet Counter Group	
Poll Data	0
Poll with No Data Sent	0
Poll replies with Data Sent	0
Poll replies with Data Sent (moreData flag set)	0
Poll replies with no data sent	0
Request for service	0
Data Process Counter Group	
Send Success	0
Send Retries	0
Send Failures	0
Receive Success	0
Receive Retries	0
Receive Failures	0
Poll no Replies	0

The **Registration Last Reason** field indicates either a successful registration (a value of 1) or it indicates the reason why the last registration failed. Possible values for the **Registration Last Reason** field are as follows:

- 1 = None (successful registration)
- 2 = Maximum number of SUs reached
- 3 = Authentication failure
- 4 = Roaming
- 5 = No response from SU within the Registration Timeout Period
- 6 = Low Signal Quality

View Number of ICMP Messages

Click **Monitor** > **ICMP** to view the number of ICMP messages sent and received by the unit. It includes **ping**, **route**, and **host unreachable** messages.

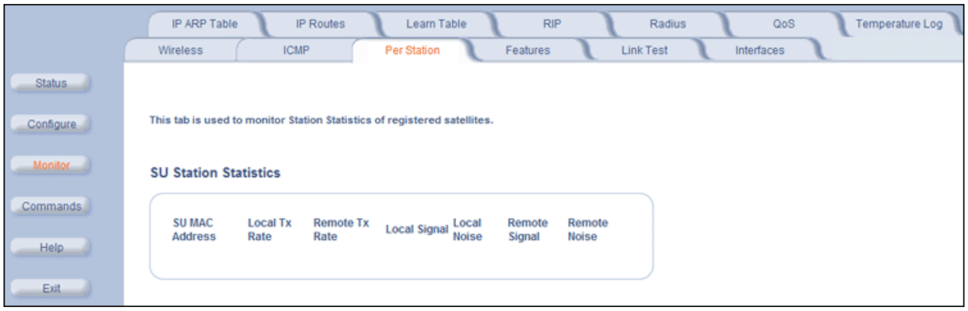


Messages Received		Messages Sent	
Total Messages	0	Total Messages	0
Errors	0	Errors	0
Destination Unreachable	0	Destination Unreachable	0
Time Exceeded	0	Time Exceeded	0
Parameter Problems	0	Parameter Problems	0
Source Quench	0	Source Quench	0
Redirects	0	Redirects	0
Echos	0	Echos	0
Echo Reply	0	Echo Reply	0
Time Stamps	0	Time Stamps	0
Time Stamp Reply	0	Time Stamp Reply	0
Address Mask	0	Address Mask	0
Address Mask Reply	0	Address Mask Reply	0

View Per Station Statistics

Click **Monitor** > **Per Station** to view Station Statistics. On the SU, the "Per Station" page shows statistics of the BSU to which the SU is registered. On the BSU, it shows statistics of all the SU's connected to the BSU.

The page's statistics refresh every 4 seconds.



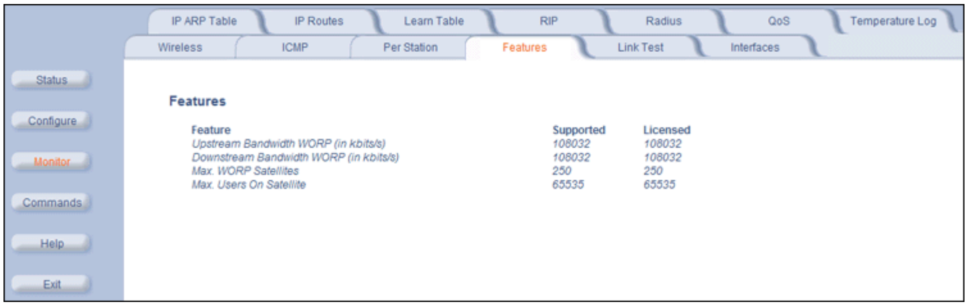
This tab is used to monitor Station Statistics of registered satellites.

SU Station Statistics

SU MAC Address	Local Tx Rate	Remote Tx Rate	Local Signal	Local Noise	Remote Signal	Remote Noise

View Features Supported

Click **Monitor** > **Features** to view the following information.



Features

Feature	Supported	Licensed
Upstream Bandwidth WORP (in kbits/s)	*108032*	*108032*
Downstream Bandwidth WORP (in kbits/s)	*108032*	*108032*
Max. WORP Satellites	*250*	*250*
Max. Users On Satellite	*65535*	*65535*

NOTE: *A BSU shows how many WORP SUs it can support; the SU shows how many Ethernet hosts it supports on its Ethernet port as the “Max Users on Satellite” parameter.*

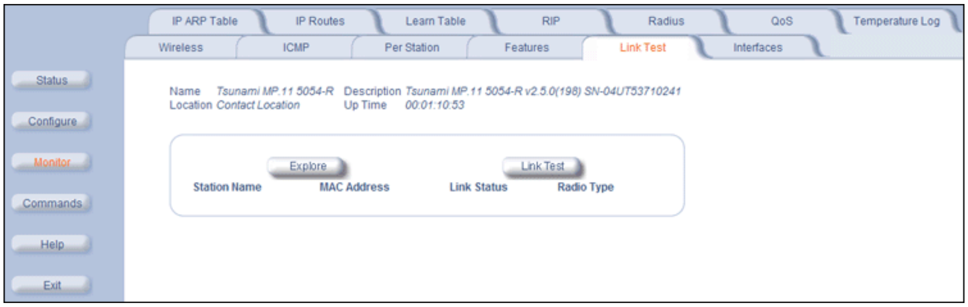
Test Link Quality

Click **Monitor** > **Link Test** to find out which wireless stations are in range and to check their link quality.

NOTE: *Link Test requires Internet Explorer version 6.0 or later. Earlier versions do not support Link Test.*

Link Test for the unit reports the Signal-to-Noise Ratio (SNR) value in dB; the higher this number, the better the signal quality. Furthermore, it reports the signal level and noise level in dBm. The latter two are approximations of the level at which the unit receives the signal of the peer unit and the background noise.

- Clicking **Explore** from a BSU displays all its registered SUs.
- Clicking **Explore** from an SU displays only the BSU with which it is registered.

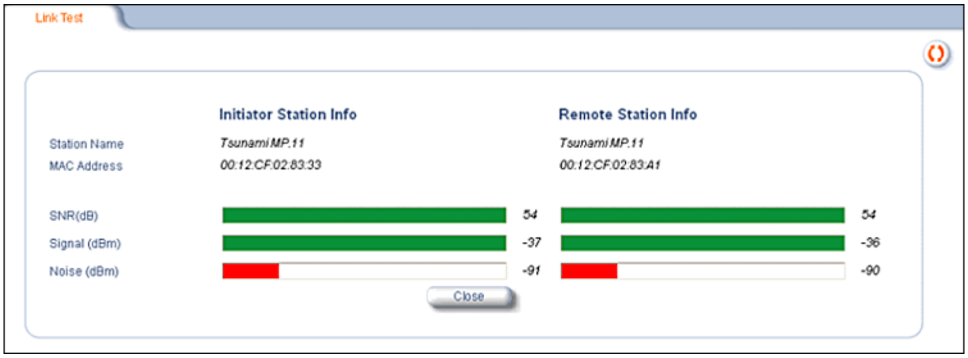


Name *Tsunami MP.11 5054-R* Description *Tsunami MP.11 5054-R v2.5.0(198) SN-04UT53710241*
Location *Contact Location* Up Time *00:01:10:53*

Station Name	MAC Address	Link Status	Radio Type

All stations displayed after “Explore” come up “Disabled.” Select a station by changing **Disabled** to **Start** and click the **Link Test** button. You can change multiple stations to **Start**, but only the last station in the list is displayed as the remote partner when you click the **Link Test** button.

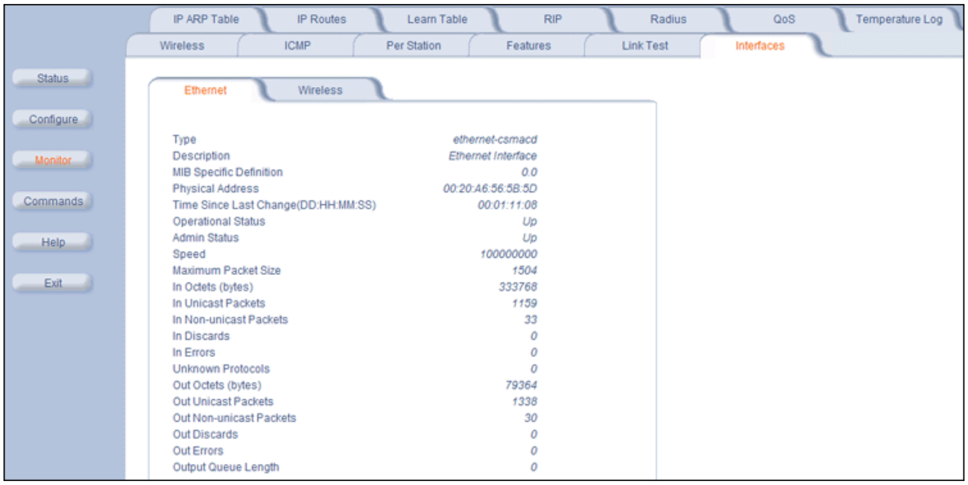
The Link Test provides SNR, Signal, and Noise information for both, the local and the remote unit’s levels. Link Test stops when you close the **Link Test** page.



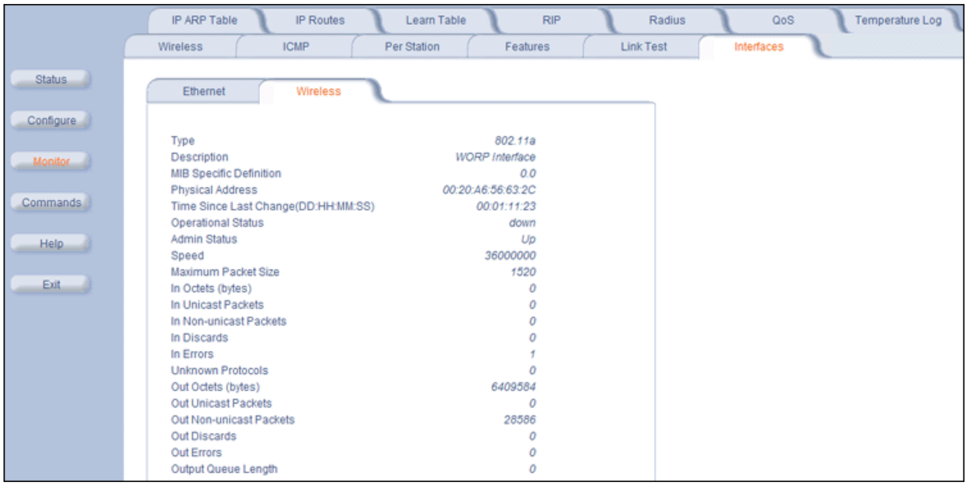
	Initiator Station Info		Remote Station Info	
Station Name	*Tsunami MP.11*		*Tsunami MP.11*	
MAC Address	*00:12:CF:02:83:33*		*00:12:CF:02:83:A1*	
SNR(dB)	🟩	54	🟩	54
Signal (dBm)	🟩	-37	🟩	-36
Noise (dBm)	🟥	-91	🟥	-90

Monitor Interfaces

Click **Monitor** > **Interfaces** to view detailed information about the IP-layer performance of the unit's interfaces. There are two sub-tabs: **Wireless** and **Ethernet**. The following figures show both interfaces.



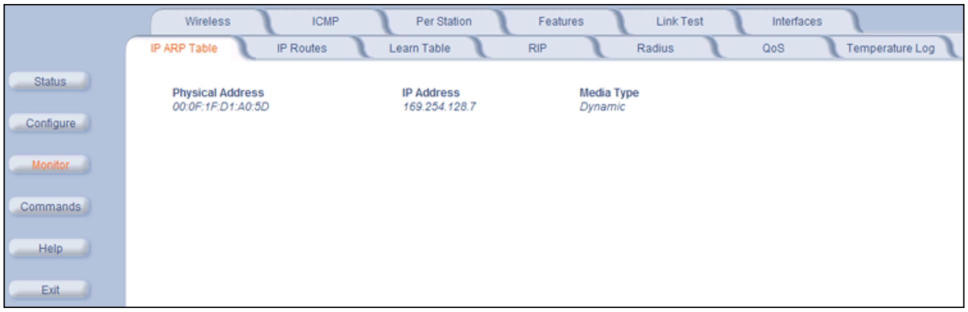
Type	*ethernet-csmacd*
Description	*Ethernet Interface*
MIB Specific Definition	*0.0*
Physical Address	*00:20:A6:56:5B:5D*
Time Since Last Change(DD:HH:MM:SS)	*00:01:11:08*
Operational Status	*Up*
Admin Status	*Up*
Speed	*100000000*
Maximum Packet Size	*1504*
In Octets (bytes)	*333768*
In Unicast Packets	*1159*
In Non-unicast Packets	*33*
In Discards	*0*
In Errors	*0*
Unknown Protocols	*0*
Out Octets (bytes)	*79364*
Out Unicast Packets	*1338*
Out Non-unicast Packets	*30*
Out Discards	*0*
Out Errors	*0*
Output Queue Length	*0*



Type	*802.11a*
Description	*WORP Interface*
MIB Specific Definition	*0.0*
Physical Address	*00:20:A6:56:63:2C*
Time Since Last Change(DD:HH:MM:SS)	*00:01:11:23*
Operational Status	*down*
Admin Status	*Up*
Speed	*36000000*
Maximum Packet Size	*1520*
In Octets (bytes)	*0*
In Unicast Packets	*0*
In Non-unicast Packets	*0*
In Discards	*0*
In Errors	*1*
Unknown Protocols	*0*
Out Octets (bytes)	*6409584*
Out Unicast Packets	*0*
Out Non-unicast Packets	*28586*
Out Discards	*0*
Out Errors	*0*
Output Queue Length	*0*

View the Mapping of IP and MAC Addresses

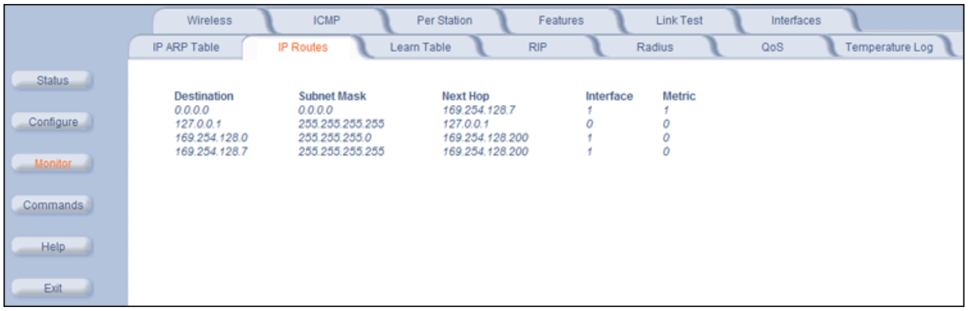
Click **Monitor** > **IP ARP Table** to view the mapping of the IP and MAC addresses of all radios registered at the BSU. This information is based upon the Address Resolution Protocol (ARP).



Physical Address	IP Address	Media Type
00:0F:1F:D1:A0:5D	*169.254.128.7*	*Dynamic*

View Active IP Routes

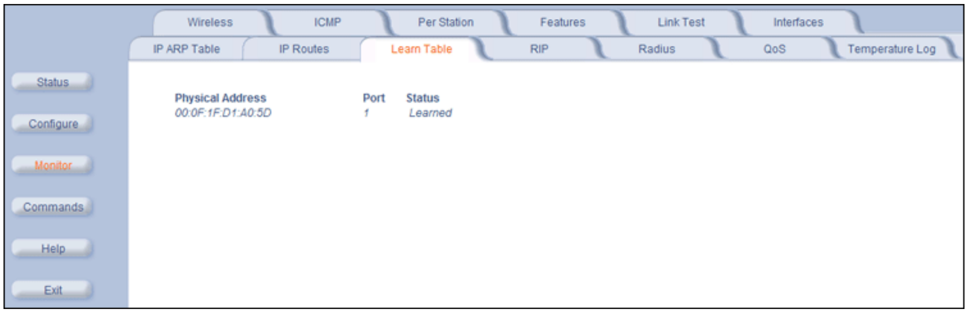
Click **Monitor** > **IP Routes** to view all active IP routes of the unit. These can be either **static** or **dynamic** (obtained through RIP). This tab is available only in **Routing** mode, and you can add routes only when in **Routing** mode.



Destination	Subnet Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	169.254.128.7	1	1
127.0.0.1	255.255.255.255	127.0.0.1	0	0
169.254.128.0	255.255.255.0	169.254.128.200	1	0
169.254.128.7	255.255.255.255	169.254.128.200	1	0

View All Detected MAC Addresses (Learn Table)

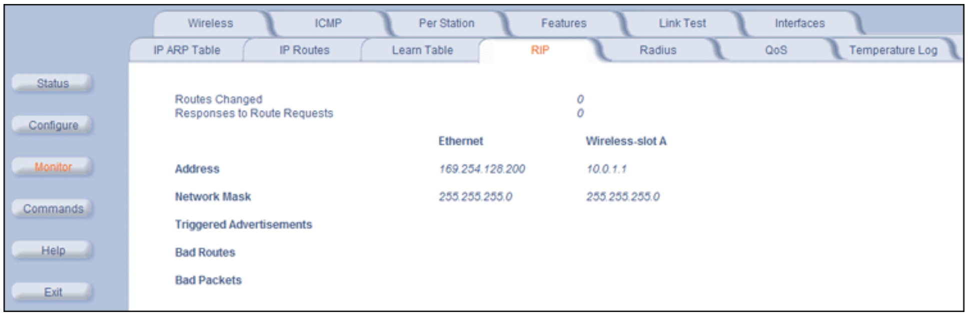
Click **Monitor** > **Learn Table** to view all MAC addresses the unit has detected on an interface. The Learn Table displays information relating to network bridging. It reports the MAC address for each node that the device has learned is on the network and the interface on which the node was detected. There can be up to 10,000 entries in the Learn Table. This tab is only available in **Bridge** mode.



Physical Address	Port	Status
00:0F:1F:D1:A0:5D	*1*	*Learned*

View RIP Data

Click **Monitor** > **RIP** to view Routing Internet Protocol data for the Ethernet and Wireless interfaces.

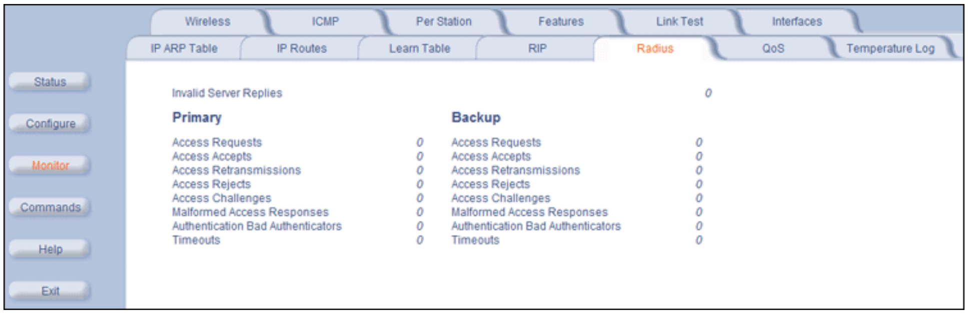


Routes Changed 0
Responses to Route Requests 0

	Ethernet	Wireless-slot A
Address	169.254.128.200	10.0.1.1
Network Mask	255.255.255.0	255.255.255.0
Triggered Advertisements		
Bad Routes		
Bad Packets		

View RADIUS Traffic Information

Click **Monitor** > **Radius** to view information about the traffic exchanged with a RADIUS server.



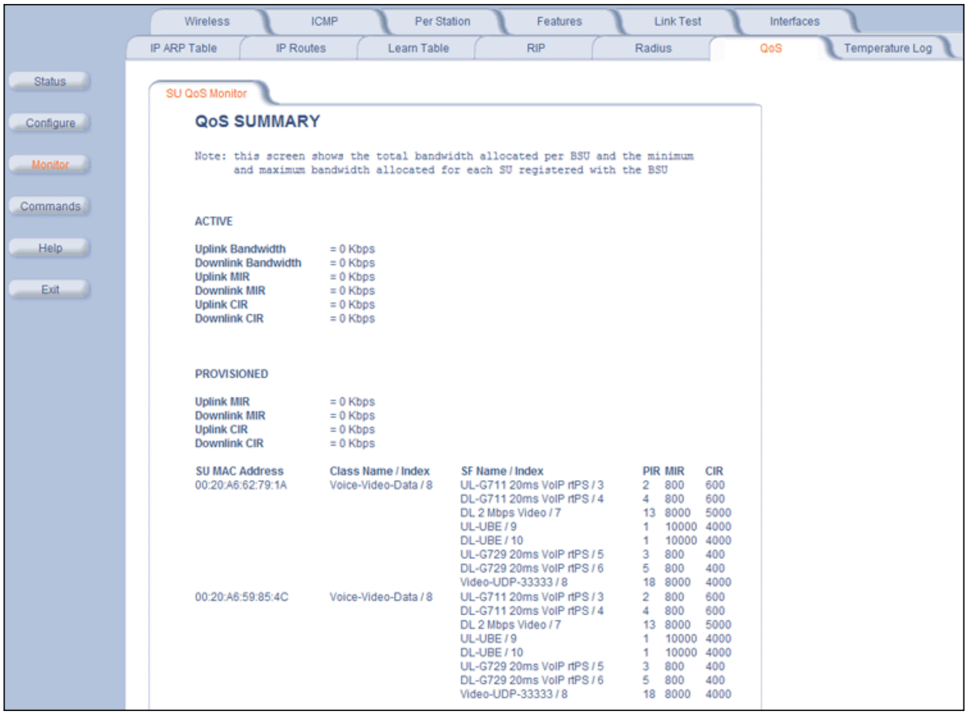
Invalid Server Replies 0

Primary		Backup	
Access Requests	0	Access Requests	0
Access Accepts	0	Access Accepts	0
Access Retransmissions	0	Access Retransmissions	0
Access Rejects	0	Access Rejects	0
Access Challenges	0	Access Challenges	0
Malformed Access Responses	0	Malformed Access Responses	0
Authentication Bad Authenticators	0	Authentication Bad Authenticators	0
Timeouts	0	Timeouts	0

View Quality of Service (QoS) Information

Click the **Monitor** button and the **QoS** tab to view summary information about the Quality of Service per BSU and for each SU registered with that BSU.

This tab is available only on the BSU.



QoS SUMMARY

```
Note: this screen shows the total bandwidth allocated per BSU and the minimum
      and maximum bandwidth allocated for each SU registered with the BSU
```

ACTIVE

Uplink Bandwidth = 0 Kbps
Downlink Bandwidth = 0 Kbps
Uplink MIR = 0 Kbps
Downlink MIR = 0 Kbps
Uplink CIR = 0 Kbps
Downlink CIR = 0 Kbps

PROVISIONED

Uplink MIR = 0 Kbps
Downlink MIR = 0 Kbps
Uplink CIR = 0 Kbps
Downlink CIR = 0 Kbps

SU MAC Address	Class Name / Index	SF Name / Index	PIR	MIR	CIR
00:20:A6:62:79:1A	Voice-Video-Data / 8	UL-G711 20ms VoIP rtPS / 3	2	800	600
		DL-G711 20ms VoIP rtPS / 4	4	800	600
		DL 2 Mbps Video / 7	13	8000	5000
		UL-UBE / 9	1	10000	4000
		DL-UBE / 10	1	10000	4000
		UL-G729 20ms VoIP rtPS / 5	3	800	400
		DL-G729 20ms VoIP rtPS / 6	5	800	400
		Video-UDP-33333 / 8	18	8000	4000
00:20:A6:59:85:4C	Voice-Video-Data / 8	UL-G711 20ms VoIP rtPS / 3	2	800	600
		DL-G711 20ms VoIP rtPS / 4	4	800	600
		DL 2 Mbps Video / 7	13	8000	5000
		UL-UBE / 9	1	10000	4000
		DL-UBE / 10	1	10000	4000
		UL-G729 20ms VoIP rtPS / 5	3	800	400
		DL-G729 20ms VoIP rtPS / 6	5	800	400
		Video-UDP-33333 / 8	18	8000	4000

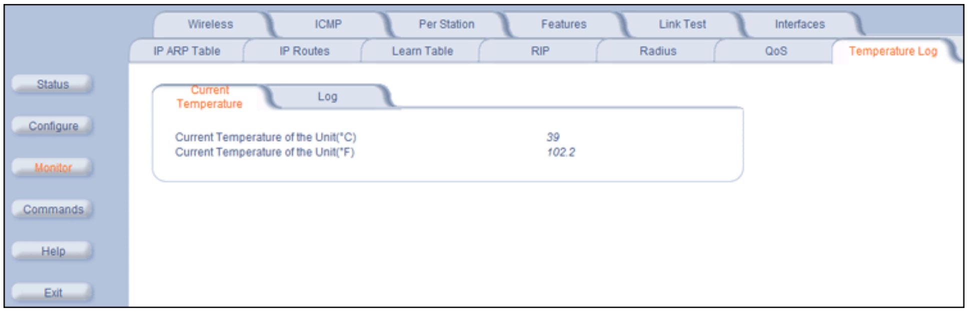
View Temperature Log

The feature for reporting and logging internal unit temperature observes and reports the internal temperature of the unit. Temperature is logged and an SNMP trap sent when the internal temperature crosses the limit of 0ºC to 55ºC (at 5 degrees before the limit, the unit issues a warning trap).

You can select a recording interval from one to sixty minutes, in 5-minute increments on the **Configure: System** tab. A log file holds the recorded data. The log can hold at least 576 entries (two days with the refresh time of 5 minutes). For further analysis, the log can be exported to a text file with a new line feed as a line separator.

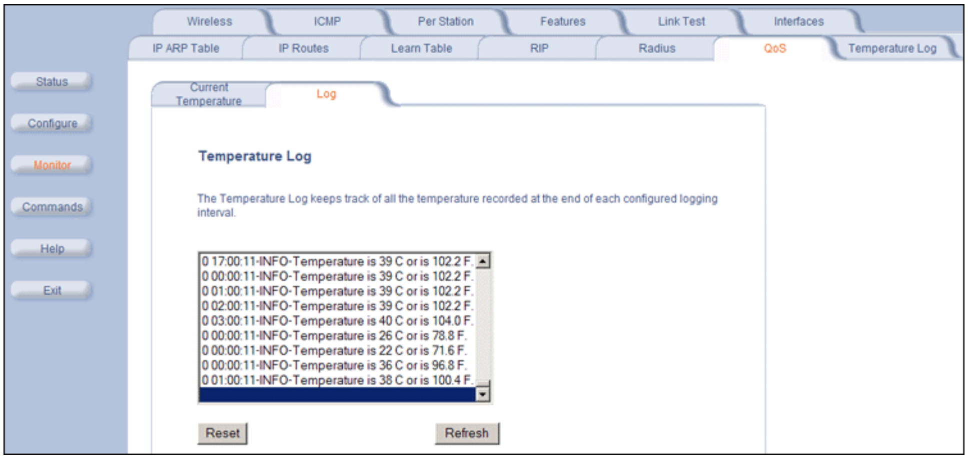
The Temperature Log contains two sub-tabs:

- The **Current Temperature** tab indicates the unit’s current temperature. The current temperature value is refreshed every 4 seconds.



Current Temperature of the Unit(°C) 39
Current Temperature of the Unit(°F) 102.2

- The **Log** tab keeps track of the temperature recorded at the end of each configured logging interval. You can reset or refresh the log using the **Reset** and **Refresh** buttons.



Temperature Log

The Temperature Log keeps track of all the temperature recorded at the end of each configured logging interval.

```
0 17:00:11-INFO-Temperature is 39 C or is 102.2 F.
0 00:00:11-INFO-Temperature is 39 C or is 102.2 F.
0 01:00:11-INFO-Temperature is 39 C or is 102.2 F.
0 02:00:11-INFO-Temperature is 39 C or is 102.2 F.
0 03:00:11-INFO-Temperature is 40 C or is 104.0 F.
0 00:00:11-INFO-Temperature is 26 C or is 78.8 F.
0 00:00:11-INFO-Temperature is 22 C or is 71.6 F.
0 00:00:11-INFO-Temperature is 36 C or is 96.8 F.
0 01:00:11-INFO-Temperature is 38 C or is 100.4 F.
```

Commands 8

This chapter describes the commands that you can issue with the Web Interface.

Click the **Commands** button to access available commands. See the following:

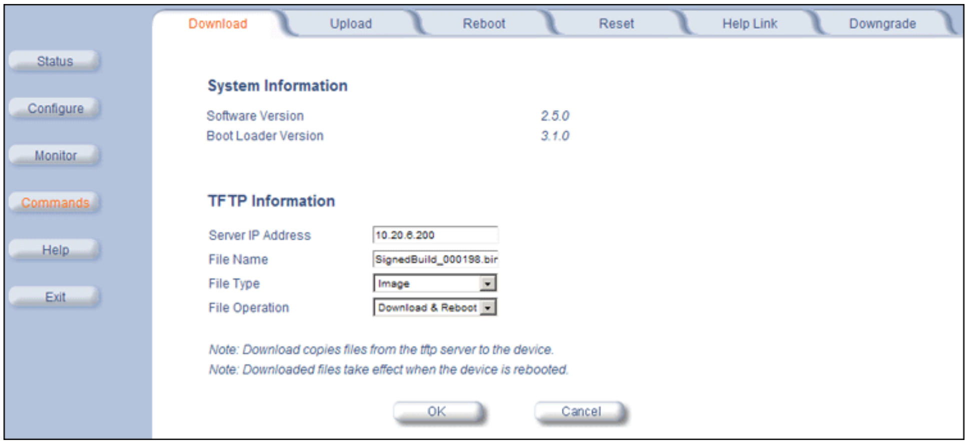
- Download (see Download Files)
- Upload (see Upload Files)
- Downgrade (see Downgrade to Previous Release)
- Reboot (see Reboot the Unit)
- Reset (see Reset the Unit to Factory Default)
- Help Link (see Set the Help Link Location)

Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

Download Files

Click **Commands** > **Download** tab to download configuration, image and license files to the unit via a TFTP server (see TFTP Server Setup for information about the SolarWinds TFTP server software located on your product installation CD).



System Information

Software Version 2.5.0

Boot Loader Version 3.1.0

TFTP Information

Server IP Address 10.20.6.200

File Name SignedBuild_000198.bir

File Type Image

File Operation Download & Reboot

Note: Download copies files from the tftp server to the device.

Note: Downloaded files take effect when the device is rebooted.

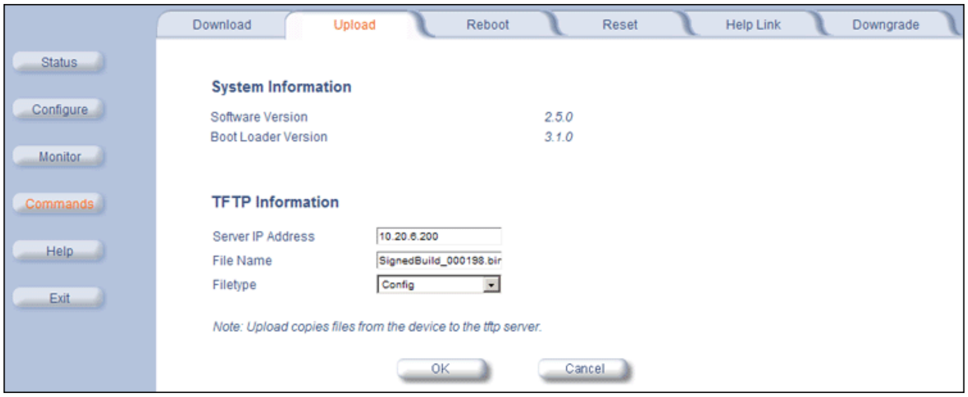
The following parameters may be configured or viewed:

- **Server IP address:** Enter the TFTP Server IP address.
- **File Name:** Enter the name of the file to be downloaded. If you are using the SolarWinds TFTP server software located on your product installation CD, the default directory for downloading files is **C:\TFTP-Root**.
- **File Type:** Choose either **Config, image, BspBl,** or **license.**
- **File Operation:** Choose either **Download** or **Download and Reboot.**

Click **OK** to start the download.

Upload Files

Click **Commands** > **Upload** to upload a configuration or log file from the unit to a TFTP server (see TFTP Server Setup for information about the SolarWinds TFTP server software located on your product installation CD).



System Information

Software Version 2.5.0
Boot Loader Version 3.1.0

TFTP Information

Server IP Address 10.20.6.200
File Name SignedBuild_000198.bir
Filetype Config

Note: Upload copies files from the device to the tftp server.

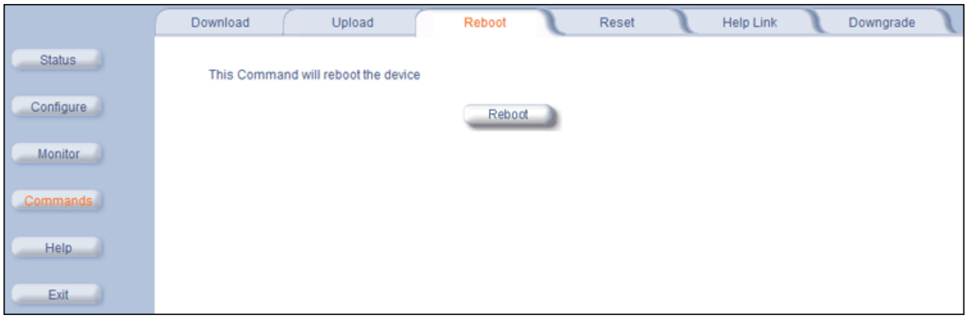
The following parameters may be configured or viewed:

- **Server IP address:** Enter the TFTP Server IP address.
- **File Name:** Enter the name of the file to be uploaded. If you are using the SolarWinds TFTP server software located on your product installation CD, the default directory for uploading files is **C:\TFTP-Root**.
- **File Type:** Choose either **Config**, **Templog**, or **Eventlog**.

Click **OK** to start the upload.

Reboot the Unit

Click **Commands** > **Reboot** to reboot the unit's embedded software. Configuration changes are saved and the unit is reset.

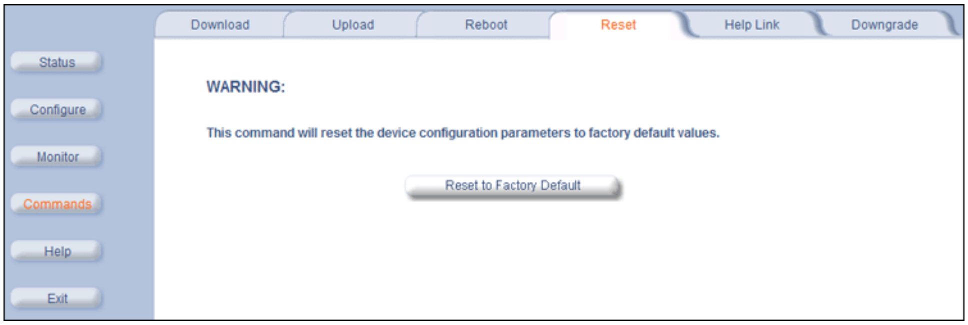


This Command will reboot the device

*<span>**CAUTION:**</span> Rebooting the unit causes all users currently connected to lose their connection to the network until the unit has completed the reboot process and resumed operation.*

Reset the Unit to Factory Default

Click **Commands** > **Reset** to restore the configuration of the unit to the factory default values.



WARNING:

This command will reset the device configuration parameters to factory default values.

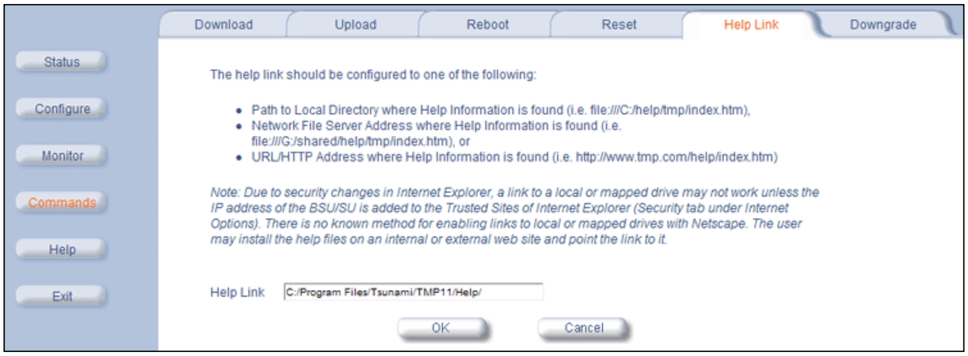
You can also reset the unit by pressing the RELOAD button located on the side of the power brick. See Hard Reset to Factory Default for more information.

CAUTION: *Resetting the unit to its factory default configuration permanently overwrites all changes made to the unit. The unit reboots automatically after this command has been issued.*

Set the Help Link Location

Click **Commands** > **Help Link** to set the location of the help files of the Web Interface. Upon installation, the help files are installed in the **C:\Program Files\Tsunami\MP.11 [Product Name]\Help** folder.

If you want to place these files on a shared drive, copy the **Help** folder to the new location and specify the new path in the **Help Link** box.



The help link should be configured to one of the following:

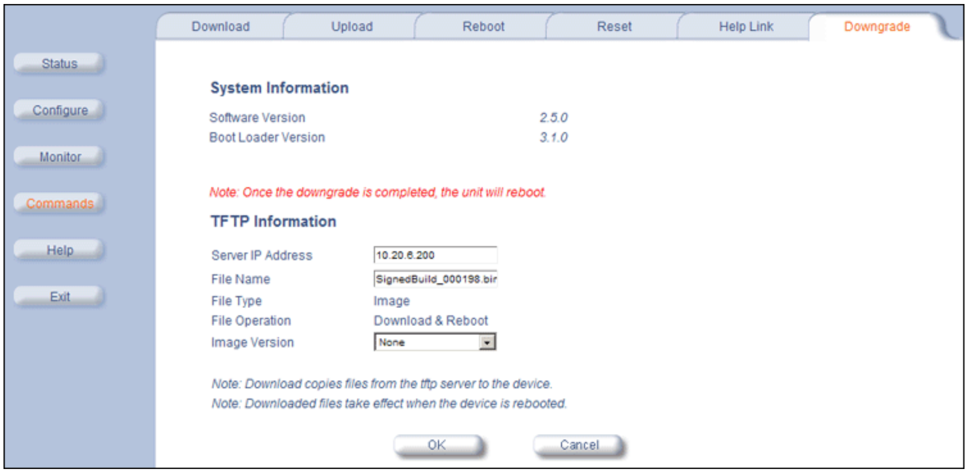
- Path to Local Directory where Help Information is found (i.e. file:///C:/help/tmp/index.htm),
- Network File Server Address where Help Information is found (i.e. file:///G:/shared/help/tmp/index.htm), or
- URL/HTTP Address where Help Information is found (i.e. http://www.tmp.com/help/index.htm)

Note: Due to security changes in Internet Explorer, a link to a local or mapped drive may not work unless the IP address of the BSU/SU is added to the Trusted Sites of Internet Explorer (Security tab under Internet Options). There is no known method for enabling links to local or mapped drives with Netscape. The user may install the help files on an internal or external web site and point the link to it.

Help Link: C:/Program Files/Tsunami/TMP11/Help/

Downgrade to Previous Release

Click **Commands** > **Downgrade** tab to downgrade to a previous release. Downgrade currently is supported only to release 2.0.1 and later. Once you enter this command, the unit is downgraded to the specified release and is automatically rebooted. The filename specified and the filename of the image selected for downgrade must be the same version. The unit will download the file, re-format the configuration to match the version, and reboot to put the image into effect.



System Information

Software Version 2.5.0
Boot Loader Version 3.1.0

Note: Once the downgrade is completed, the unit will reboot

TFTP Information

Server IP Address 10.20.6.200
File Name SignedBuild_000198.bir
File Type Image
File Operation Download & Reboot
Image Version None

Note: Download copies files from the tftp server to the device.
Note: Downloaded files take effect when the device is rebooted.

Procedures 9

This chapter describes the following procedures:

- TFTP Server Setup: Prepares the TFTP server for transferring files to and from the unit. This procedure is used by the other procedures that transfer files.
- Web Interface Image File Download: Upgrades the embedded software.
- Configuration Backup: Saves the configuration of the unit.
- Configuration Restore: Restores a previous configuration through configuration file download.
- Soft Reset to Factory Default: Resets the unit to the factory default settings through the Web or Command Line Interface.
- Hard Reset to Factory Default: In some cases, it may be necessary to revert to the factory default settings (for example, if you cannot access the unit or you lost the password for the Web Interface).
- Forced Reload: Completely resets the unit and erases the embedded software. Use this procedure only as a last resort if the unit does not boot and the “Hard Reset to Factory Default” procedure did not help. If you perform a Forced Reload, you must download a new image file as described in Image File Download with the Bootloader.
- Image File Download with the Bootloader: If the unit does not contain embedded software, or the embedded software is corrupt, you can use this procedure to download a new image file.

TFTP Server Setup

A Trivial File Transfer Protocol (TFTP) server lets you transfer files across a network. You can upload files from the unit for backup or copying, and you can download the files for configuration and image upgrades. The SolarWinds TFTP server software is located on the product installation CD, or can be downloaded from http://support.proxim.com. You can also download the latest TFTP software from SolarWind's Web site at http://www.solarwinds.net. **The instructions that follow assume that you are using the SolarWinds TFTP server software**; other TFTP servers may require different configurations.

NOTE: *If a TFTP server is not available in the network, you can perform similar file transfer operations using the HTTP interface.*

To download or upload a file, you must connect to the computer with the TFTP server through the unit's Ethernet port. This can be any computer in the network or a computer connected to the unit with a cross-over Ethernet cable. For information about installing the TFTP server, see Step 9: Install Documentation and Software.

Ensure that:

1. The upload or download directory is correctly set (the default directory is **C:\TFTP-Root**).
2. The required image file is present in the directory.
3. The TFTP server is running. ***The TFTP server must be running only during file upload and download.*** You can check the connectivity between the unit and the TFTP server by pinging the unit from the computer that hosts the TFTP server. The ping program should show replies from the unit.
4. The TFTP server is configured to both Transmit and Receive files (on the **Security** tab under **File** > **Configure**), with no automatic shutdown or time-out (on the **Auto-Close** tab).

Web Interface Image File Download

In some cases, it may be necessary to upgrade the embedded software of the unit by downloading an image file. To download an image file through the Web Interface:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in Logging in to the Web Interface.
3. Click **Commands** > **Download** tab.
4. Fill in the following details:
   - **Server IP Address** <IP address TFTP server>
   - **File Name** <image file name>
   - **File Type** Image
   - **File Operation** Download
5. Click **OK** to start the file transfer.

The unit downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the unit is ready to start the embedded software upon reboot.

Configuration Backup

You can back up the unit's configuration by uploading the configuration file. You can use this file to restore the configuration or to configure another unit (see Configuration Restore).

To upload a configuration file through the Web Interface:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in Logging in to the Web Interface.
3. Click **Commands** > **Upload**.
4. Fill in the following details:
   - **Server IP Address** <IP address TFTP server>
   - **File Name** <configuration file name>
   - **File Type** Config
   - **File Operation** Upload
5. Click **OK** to start the file transfer.

The unit uploads the configuration file. The TFTP server program should show upload activity after a few seconds. When the upload is complete, the configuration is backed up.

Configuration Restore

You can restore the configuration of the unit by downloading a configuration file. The configuration file contains the configuration information of a unit.

To download a configuration file through the Web Interface:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in Logging in to the Web Interface.
3. Click **Commands** > **Download** tab.
4. Fill in the following details:
   - **Server IP Address** <IP address TFTP server>
   - **File Name** <configuration file name>
   - **File Type** Config
   - **File Operation** Download
5. Click **OK** to start the file transfer.

The unit downloads the configuration file. The TFTP server program should show download activity after a few seconds. When the download is complete and the system rebooted, the configuration is restored.

Soft Reset to Factory Default

If necessary, you can reset the unit to the factory default settings. Resetting to default settings means that you must configure the unit anew.

To reset to factory default settings using the Web Interface:

1. Click the **Commands** button and the **Reset** tab.
2. Click the **Reset to Factory Default** button.

The device configuration parameter values are reset to their factory default values.

If you do not have access to the unit, you can use the procedure described in “Hard Reset to Factory Default” below as an alternative.

Hard Reset to Factory Default

If you cannot access the unit or you have lost its password, you can reset the unit to the factory default settings. Resetting to default settings means you must configure the unit anew.

To reset to factory default settings, press and hold the RELOAD button on the side of the unit's power supply for a minimum of 5 seconds but no more than 10 seconds. The configuration is deleted from the unit and the unit reboots, writing and using a default configuration.

CAUTION: *It you hold the RELOAD button for longer than 20 seconds, you may go into* Forced Reload *mode, which erases the unit's embedded software. This software image must be reloaded through an Ethernet connection with a TFTP server. The image filename to be downloaded can be configured with either ScanTool through the Ethernet interface or with the Boot Loader CLI through the serial port to make the unit functional again.*

Forced Reload

With Forced Reload, you erase the embedded software. Use this procedure only as a last resort if the unit does not boot and the “Reset to Factory Defaults” procedure did not help. If you perform a Forced Reload, you must download a new image file with the Boot Loader (see “Image File Download with the Boot Loader” below).

CAUTION: *The following procedure erases the embedded software of the unit. This software image must be reloaded through an Ethernet connection with a TFTP server. The image filename to be downloaded can be configured with ScanTool through the Ethernet interface to make the unit functional again.*

To do a forced reload:

1. Disconnect and reconnect power to the unit; the unit resets and the LEDs flash.
2. Immediately press and hold the RELOAD button on the side of the unit’s power supply for about 20 seconds. The software image and configuration are deleted from the unit.
3. Follow the Image File Download with the Bootloader procedure to download an image file.

Image File Download with the Bootloader

The following procedures download an image file to the unit after the embedded software has been erased with Forced Reload or when the embedded software cannot be started by the Bootloader. A new image file can be downloaded to the unit with ScanTool, or the Command Line Interface through the unit's serial port. In both cases, the file is transferred through Ethernet with TFTP. Because the CLI serial port option requires a serial RS-232C cable, Proxim recommends the ScanTool option.

Download with ScanTool

To download an image file with the ScanTool:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Run ScanTool on a computer that is connected to the same LAN subnet as the unit. ScanTool scans the subnet for units and displays the found units in the main window. If in Forced Reload, ScanTool does not find the device until the unit Bootloader times out from its default operation to download an image. Click **Rescan** to re-scan the subnet and update the display until the unit shows up in Bootloader mode.
3. Select the unit to which you want to download an image file and click Change.
4. Ensure that **IP Address Type Static** is selected and fill in the following details:
   - Password
   - IP Address and Subnet Mask of the unit.
   - **TFTP Server IP Address** and, if necessary, the **Gateway IP Address** of the TFTP server.
   - **Image File Name** of the file with the new image.
5. Click **OK** to start the file transfer.

The unit downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the LED pattern should return to **reboot** state. The unit is ready to start the embedded software.

After a Forced Reload procedure, the unit returns to factory default settings and must be reconfigured. ScanTool can be used to set the system name and IP address.

To access the unit, see Logging in to the Web Interface.

Download with CLI

To use the CLI through the serial port of the unit, you need a connector cable with a male RJ11 and a female DB9 connector (included with the unit) and an ASCII terminal program such as HyperTerminal. Proxim recommends you switch off the unit and the computer before connecting or disconnecting the serial RS-232C cable.

To download an image file:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Start the terminal program (such as HyperTerminal), set the following connection properties, and then connect:
   - COM port: for example, COM1 or COM2 to which the unit serial port is connected)
   - Bits per second: 9600
   - Data bits 8
   - Stop bits: 1
   - Flow control: None
   - Parity: None
3. Disconnect and reconnect power to reset the unit; the terminal program displays Power On Self Test (POST) messages.

4. When the **"Sending Traps to SNMP manager periodically**" message is displayed (after about 30 seconds), press the **ENTER** key.
5. The command prompt is displayed; enter the following commands:

```
set ipaddr <IP address nit>
set ipsubmask <subnet mask>
set ipaddrtype static
set tftpipaddr <IP address TFTP server>
set tftpfilename <image file name>
set ipgw <gateway IP address>
reboot
```

For example:

```
set ipaddr 10.0.0.12
set ipsubmask 255.255.255.0
set ipaddrtype static
set tftpipaddr 10.0.0.20
set tftpfilename image.bin
set ipgw 10.0.0.30
reboot
```

The unit reboots and downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the unit is ready for configuration.

To access the unit, see Logging in to the Web Interface. Note that the IP configuration in normal operation differs from the IP configuration of the Boot Loader.

Troubleshooting 10

This chapter helps you to isolate and solve problems with your unit. In the event this chapter does not provide a solution, or the solution does not solve your problem, check our support website at http://support.proxim.com.

Before you start troubleshooting, it is important that you have checked the details in the product documentation. For details about RADIUS, TFTP, terminal and telnet programs, and Web browsers, refer to their appropriate documentation.

In some cases, rebooting the unit clears the problem. If nothing else helps, consider a Soft Reset to Factory Default or a Forced Reload. The Forced Reload option requires you to download a new image file to the unit.

See the following:

- Connectivity Issues
- Communication Issues
- Setup and Configuration Issues
- VLAN Operation Issues
- Link Problems

Connectivity Issues

The issues described in this section relate to the connections of the unit.

Unit Does Not Boot

The unit shows no activity (the power LED is off).

1. Ensure that the power supply is properly working and correctly connected.
2. Ensure that all cables are correctly connected.
3. Check the power source.
4. If you are using an Active Ethernet splitter, ensure that the voltage is correct.

Serial Link Does Not Work

The unit cannot be reached through the serial port.

1. Check the cable connection between the unit and the computer.
2. Ensure that the correct COM port is used.
3. Start the terminal program; set the following connection properties (also see “HyperTerminal Connection Properties” in the *Tsunami MP.11 Reference Manual*), and then connect.
   - COM port: for example, COM1 or COM2 to which the unit serial port is connected)
   - Bits per second: 9600
   - Data bits 8
   - Stop bits: 1
   - Flow control: None
   - Parity: None
4. Ensure that the unit and the computer use the same serial port configuration parameters.
5. Disconnect and reconnect power to reset the unit. The terminal program displays Power On Self Tests (POST) messages and displays the following after approximately 90 seconds: **`Please enter password`**:

HyperTerminal Connection Problems

The serial connection properties can be found in HyperTerminal as follows:

1. Start HyperTerminal and select Properties from the File menu.
2. Select **Direct to Com 1** in the **Connect using**: drop-down list (depending upon the COM port you use); then click **Configure**. A window such as the following is displayed:
3. Enter or edit the information as follows, and click **OK**.
   - Bits per second: 9600
   - Data bits 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
4. Click the **Settings** tab and then click **ASCII Setup…**. A window similar to the following is displayed:
5. Ensure that Send line ends with line feeds is selected and click OK twice. HyperTerminal is now correctly configured.

Ethernet Link Does Not Work

1. First check the Ethernet LED:
   - Solid Green: Power is on, the radio is up, and the Ethernet link is also up.
   - Blinking Green: Power is on, the radio is coming up and the Ethernet is down.
2. Verify pass-through versus cross-over cable.

Cannot Use the Web Interface

1. Open a command prompt window and enter **`ping <ip address unit>`** (for example **`ping 10.0.0.1`**). If the unit does not respond, make sure that you have the correct IP address.
   If the unit responds, the Ethernet connection is working properly, continue with this procedure.
2. Ensure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later (Version 6.0 or later recommended)
   - Netscape version 6.0 or later.
3. Ensure that you are not using a proxy server for the connection with your Web browser.
4. Ensure that you have not exceeded the maximum number of Web Interface or CLI sessions.
5. Double-check the physical network connections. Use a well-known unit to ensure the network connection is properly functioning.
6. Perform network infrastructure troubleshooting (check switches, routers, and so on).

Communication Issues

Two Units Are Unable to Communicate Wirelessly

If a wireless link is possible after testing two units within close distance of each other, then there are two possible reasons why wireless connectivity is not possible while the MP.11 units are at their desired locations:

1. There may be a problem in the RF path, for example, a bad connector attachment (this is the most common problem in installations) or a bad cable (water ingress).

   NOTE: *The cables can be swapped with known good ones as a temporary solution to verify cable quality.*

2. Another reason may be related to an interference problem caused by a high signal level from another radio. This can be checked by changing the frequency and then verifying whether another channel works better or by changing the polarization as a way of avoiding the interfering signal. To know in advance how much interference is present in a given environment, a Spectrum Analyzer can be attached to a (temporary) antenna for measuring the signal levels on all available Channels.

NOTE: *The antennas are usually not the problem, unless mounted upside down causing the drain hole to be quickly filled with radome.*

If a wireless link is not possible after testing two units within close distance of each other, then the problem is either hardware or configuration related, such as a wrong Network name, Encryption key, Network Secret or Base Station Name. To eliminate these issues from being a factor, resetting the both units to factory defaults is the recommended solution.

If a wireless link is not possible after resetting the units and verifying that one unit is a BSU with WORP Base interface configured and the other is a Satellite, then the problem is not configuration related and the only remaining reason is a possible hardware problem. Acquiring a third unit and then testing it amongst the existing units will help pinpoint the broken unit.

Setup and Configuration Issues

The following issues relate to setup and configuration problems.

Lost Password

If you lost your password, you must reset the unit to the default settings. See Hard Reset to Factory Default. The default password is **public**.

If you record your password, keep it in a safe place.

The Unit Responds Slowly

If the unit takes a long time to become available, it could mean that:

- No DHCP server is available.
- The IP address of the unit is already in use.

  Verify that the IP address is assigned only to the unit. Do this by switching off the unit and then pinging the IP address. If there is a response to the ping, another device in the network is using the same IP address. If the unit uses a static IP address, switching to DHCP mode could remedy this problem. Also see Setting the IP Address with ScanTool.
- There is too much network traffic.

Web Interface Does Not Work

If you cannot connect to the unit Web server through the network:

1. Connect a computer to the serial port of the unit and check the HTTP status. The HTTP status can restrict HTTP access at different interfaces. For more information, see “Serial Port” in the *Tsunami MP.11 Reference Manual*.
2. Open a command prompt window and enter: **`ping <ip address unit>`** (for example **`ping`** `10.0.0.1`)
   - If the unit does not respond, ensure that you have the correct IP address.
   - If the unit responds, the Ethernet connection is working properly; continue with this procedure.
3. Ensure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later (Version 6.0 or later recommended)
   - Netscape version 6.0 or later
4. Ensure that you are not using a proxy server for the connection with your Web browser.
5. Ensure that you have not exceeded the maximum number of Web Interface sessions.

Command Line Interface Does Not Work

If you cannot connect to the unit through the network:

1. Connect a computer to the serial port of the unit and check the SNMP table. The SNMP table can restrict telnet or HTTP access. For more information, see “Serial Port” in the *Tsunami MP.11 Reference Manual*.
2. Open a command prompt window and enter: **`ping`** `<ip address unit>` (for example **`ping 10.0.0.1`**).
   - If the unit does not respond, ensure that you have the correct IP address.
   - If the unit responds, the Ethernet connection is working properly; continue with this procedure.
3. Ensure that you have not exceeded the maximum number of CLI sessions.

TFTP Server Does Not Work

With TFTP, you can transfer files to and from the unit. Also see TFTP Server Setup. If a TFTP server is not properly configured and running, you cannot upload and download files. The TFTP server:

- Can be situated either local or remote
- Must have a valid IP address
- Must be set for send and receive without time-out
- Must be running only during file upload and download

If the TFTP server does not upload or download files, it could mean:

- The TFTP server is not running
- The IP address of the TFTP server is invalid
- The upload or download directory is not correctly set
- The file name is not correct

Online Help Is Not Available

Online help is not available:

1. Make sure that the Help files are installed on your computer or server. Also see Step 9: Install Documentation and Software.
2. Verify whether the path of the help files in the Web Interface refers to the correct directory. See Set the Help Link Location.

Changes Do Not Take Effect

Changes made in the Web Interface do not take effect:

1. Restart your Web browser.
2. Log into the radio unit again and make changes.
3. Reboot the radio unit when prompted to do so.

Wait until the reboot is completed before accessing the unit again.

VLAN Operation Issues

The correct VLAN configuration can be verified by "pinging" wired hosts from both sides of the device and the network switch. Traffic can be "sniffed" on the wired (Ethernet) network.   Packets generated by hosts and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers when in Transparent mode. The VLAN ID in the headers should correspond to one of the VLAN Management IDs configured for the unit in Trunk mode.

The correct VLAN assignment can be verified by pinging:

- The unit to ensure connectivity
- The switch to ensure VLAN properties
- Hosts past the switch to confirm the switch is functional

Ultimately, traffic can be "sniffed" on the Ethernet interface using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the assigned VLAN.

What if network traffic is being directed to a nonexistent host?

- All sessions are disconnected, traffic is lost, and a manual override is necessary.
- Workaround: You can configure the switch to mimic the nonexistent host.

Link Problems

While wireless networking emerges more and more, the number of wireless connections to networks grows every day. The Tsunami MP.11 unit is one of the successful product families used by customers today who enjoy the day after day high-speed, cost-effective connections. To successfully use the connections, technicians must be able to troubleshoot the system effectively. This section gives hints on how a unit network could be analyzed in the case of “no link,” a situation in which the customer thinks that the link is down because there is no traffic being passed.

The four general reasons that a wireless link may not work are related to:

- Hardware
- Configuration
- Path issues (such as distance, cable loss, obstacles)
- Environment (anything that is outside the equipment and not part of the path itself)

You have tested the equipment in the office and have verified that the hardware and configurations are sound. The path calculation has been reviewed, and the path has been double-checked for obstacles and canceling reflections. Still, the user reports that the link does not work.

Most likely, the problem reported is caused by the environment or by improper tests to verify the connection. This article assumes that the test method, cabling, antennas, and antenna alignment have been checked. Always do this before checking the environment.

General Check

Two general checks are recommended before taking any action:

- Check whether the software version at both sides is the most current
- Check for any reported alarm messages in the Event Log

Statistics Check

Interference and other negative environment factors always have an impact on the number of correctly received frames. The Tsunami MP.11 models give detailed information about transmission errors in the Web interface, under **Monitor**.

The windows that are important for validating the health of the link are:

- **Monitor / Wireless / General (Lowest level of the wireless network):** Check FCS errors: Rising FCS errors indicate interference or low fade margin. So does **Failed count**. If only one of those is high, this indicates that a source of interference is significant near one end of the link.
- **Monitor / Interfaces / Wireless (One level higher than Wireless / General):** The information is given after the wireless Ethernet frame is converted into a normal Ethernet frame. The parameters shown are part of the MIB-II.
  - Both operational and admin status should be **up**. An admin status of **down** indicates that the interface is configured to be down.
  - **In Discards** and **Out Discards** indicate overload of the buffers, likely caused by network traffic, which is too heavy.
  - **In Errors** and **Out Errors** should never happen; however, it might happen if a frame’s FCS was correct while the content was still invalid.
- **Monitor / Wireless / WORP (Statistics on WORP):** WORP runs on top of normal Ethernet, which means that the WORP frame is in fact the data field of the Ethernet frame. **Send Failure** or **Send Retries** must be low in comparison to **Send Success**. **Low** is about 1%. The same applies for **Receive Success** versus **Receive Retries** and **Receive Failures**. Note that the **Receive Failures** and **Retries** can be inaccurate. A frame from the remote site might have been transmitted without even being received; therefore, the count of that frame might not have been added to the statistics and the receiver simply could not know that there was a frame.

- **Remote Partners** indicates how many SUs are connected (in case of a BSU) or whether a Base is connected (in case of a Subscriber).
- **Base Announces** should increase continuously.
- **Registration Requests** and **Authentication Requests** should be divisible by 3. WORP is designed in a way that each registration sequence starts with 3 identical requests. It is not a problem if, once in a while, one of those requests is missing. Missing requests frequently is to be avoided.

- **Monitor / Per Station (Information per connected remote partner):** Check that the received signal level (RSL) is the same on both sides; this should be the case if output power is the same. Two different RSLs indicate a broken transmitter or receiver. A significant difference between Local Noise and Remote Noise could indicate a source of interference near the site with the highest noise. Normally, noise is about –80 dBm at 36 Mbps. This number can vary from situation to situation, of course, also in a healthy environment.
- **Monitor / Link Test (Information used by Administrators for on-the-spot checking):** Check the received signal level (RSL) and noise level. Compare the RSL with the values from path analysis. If the figures differ significantly from the values recorded at the Per Station window, check for environment conditions that change over time.

Analyzing the Spectrum

The ultimate way to discover whether there is a source of interference is to use a spectrum analyzer. Usually, the antenna is connected to the analyzer when measuring. By turning the antenna 360 degrees, one can check from which direction the interference is coming. The analyzer will also display the frequencies and the level of signal is detected.

Proxim recommends performing the test at various locations to find the most ideal location for the equipment.

Avoiding Interference

When a source of interference is identified and when the level and frequencies are known, the next step is to avoid the interference. Some of the following actions can be tried:

- Changing the channel to a frequency away from the interference is the first step in avoiding interference. For countries that require DFS, it might be not possible to manually select a different frequency.
- Each antenna has a polarization; try to change to a polarization different from the interferer.
- A small beam antenna looks only in one particular direction. Because of the higher gain of such an antenna, lowering the output power or adding extra attenuation might be required to stay legal. This solution cannot help when the source of interference is right behind the remote site.
- Lowering the antennas can help avoid seeing interference from far away.

Move the antennas to a different location on the premises. This causes the devices to look from a different angle, causing a different pattern in the reception of the signals. Use obstructions such as buildings, when possible, to shield from the interference.

Conclusion

A spectrum analyzer can be a great help to identify whether interference might be causing link problems on Tsunami MP.11 systems.

Before checking for interference, the link should be verified by testing in an isolated environment, to make sure that hardware works and your configurations are correct. The path analysis, cabling and antennas should be checked as well.

Statistics in the web interface under Monitor tell if there is a link, if the link is healthy, and a continuous test can be done using the Link Test.

Country Codes and Channels A

In the CLI and MIB browser, the country code is set using the string code, as shown in the following example.

Example: To set Taiwan as the country:

```
set syscountrycode tw
```

The following tables contain information on frequency band availability, DFS requirements (802.11a only), and allowed channels/center frequencies for specific countries. Transmit Power Control is available for all countries. See the following tables:

- Model 2454-R (2.4 GHz) Channels/Frequencies by Country
- Model 5054-R (2.4 GHz) Channels/Frequencies by Country

Model 2454-R (2.4 GHz) Channels/Frequencies by Country

Country Code	Frequency Band	Allowed Channels (Center Frequency) for 5 MHz, 10 MHz, and 20 MHz
Albenia (AL)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Algeria (DZ)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Argentina (AR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Armenia (AM)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Australia (AU)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Austria (AT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Azerbaijan (AZ)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Bahrain (BH)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Belarus (BY)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Belgium (BE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Belize (BZ)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Bolivia (BO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Brazil (BR),	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Brunei Darussalam (BN)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Bulgaria (BG)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Canada (CA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
China (CN)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Colombia (CO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)

Country Code	Frequency Band	Allowed Channels (Center Frequency) for 5 MHz, 10 MHz, and 20 MHz
Costa Rica (CR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Croatia (HR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Cyprus (CY)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Denmark (DK)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Dominican Republic (DO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
Egypt (EG)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
El Salvador (SV)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Estonia (EE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Finland (FI)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
France (FR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Georgia (GE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Germany (DE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Greece (GR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Guatemala (GT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
Honduras (HN)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Hong Kong (HK)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Hungary (HU)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Iceland (IS)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
India (IN)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Indonesia (ID)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Iran (IR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Ireland (IE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Israel (IL)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Italy (IT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Japan (JP)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Jordon (JO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Kazakhstan (KZ)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Korea Republic (KR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Kuwait (KW)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)

Country Code	Frequency Band	Allowed Channels (Center Frequency) for 5 MHz, 10 MHz, and 20 MHz
Latvia (LV)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Lebanon (LB)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Liechtenstein (LI)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Lithuania (LT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Luxembourg (LU)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Macau (MO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Macedonia (MK)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Malaysia (MY)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Malta (MT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Mexico (MX)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
Monaco (MC)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Morocco (MA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Netherlands (NL)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
New Zealand (NZ)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
North Korea (KP)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Norway (NO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Oman (OM)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Pakistan (PK)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Panama (PA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
Peru (PE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Philippines (PH)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Poland (PL)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Portugal (PT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Puerto Rico (PR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
Quatar (QA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Romania (RO)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Russia (RU)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Saudia Arabia (SA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Singapore (SG)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)

Country Code	Frequency Band	Allowed Channels (Center Frequency) for 5 MHz, 10 MHz, and 20 MHz
Slovak Republic (SK)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Slovenia (SI)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
South Africa (ZA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Spain (ES)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Sweden (SE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Switzerland (CH)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Syria (SY)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Taiwan (TW)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Thailand (TH)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Trinidad and Tobago (TT)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Tunisia (TN)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Turkey (TR)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Ukraine (UA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Ukraine (UA)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
United Arab Emirates (AE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
United Kingdom (GB)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Uruguay (UY)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
USA (US)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462)
Uzbekistan (UZ)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Vietnam (VN)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Yemen (YE)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)
Zimbabwe (ZW)	2.4 GHz	**1** (2412), **2** (2417), **3** (2422), **4** (2427), **5** (2432), **6** (2437), **7** (2442), **8** (2447), **9** (2452), **10** (2457), **11** (2462), **12** (2467), **13** (2472)

Model 5054-R (2.4 GHz) Channels/Frequencies by Country

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	10 MHz	5 MHz
Argentina (AR)	5.25 - 5.35 GHz and 5.725 - 5.825 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)	**56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805)	**56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	**10 MHz**	**5 MHz**
Australia (AU)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Austria (AT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Belgium (BE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Belize (BZ)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Bolivia (BO)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Brazil (BR)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)

Country (Code)	**Frequency Bands**	**DFS**	**Allowed Channels (Center Freq)**		
			20 MHz	**10 MHz**	**5 MHz**
Brazil1 (BR1)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Brunei Darussalam (BN)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Bulgaria (BG)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Canada (CA)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
China (CN)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Colombia (CO)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)

Country (Code)	**Frequency Bands**	**DFS**	**Allowed Channels (Center Freq)**		
			20 MHz	**10 MHz**	**5 MHz**
Cyprus (CY)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Denmark (DK)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Dominican Republic (DO)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Estonia (EE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)

Country (Code)	**Frequency Bands**	**DFS**	**Allowed Channels (Center Freq)**		
			20 MHz	**10 MHz**	**5 MHz**
Finland (FI)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
France (FR)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Germany (DE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Greece (GR)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)

Country (Code)	**Frequency Bands**	**DFS**	**Allowed Channels (Center Freq)**		
			20 MHz	**10 MHz**	**5 MHz**
Guatemala (GT)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Hong Kong (HK)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Hungary (HU)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Iceland (IS)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
India (IN)	5.15 - 5.35 GHz and 5.725 - 5.825 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240), **52** (5260), **56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)	**36** (5180), **38** (5190), **40** (5200), **42** (5210), **44** (5220), **46** (5230), **48** (5240), **50** (5250), **52** (5260), **54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**36** (5180), **37** (5185), **38** (5190), **39** (5195), **40** (5200), **41** (5205), **42** (5210), **43** (5215), **44** (5220), **45** (5225), **46** (5230), **47** (5235), **48** (5240), **49** (5245), **50** (5250), **51** (5255), **52** (5260), **53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	10 MHz	5 MHz
Iran (IR)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Ireland (IE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Ireland 5.8 GHz (IE1)	5.725 - 5.85 GHz	Yes	**147** (5735), **151** (5755), **155** (5775), **167** (5835)	**145** (5725), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **163** (5815), **165** (5825), **167** (5835), **169** (5845)	**145** (5725), **146** (5730), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835), **168** (5840), **169** (5845), **170** (5850)
Italy (IT)	5.47 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Japan (JP)	5.25 - 5.35 GHz	Yes	**56** (5280), **60** (5300), **64** (5320)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335)
Japan1 (JP1)	5.15 - 5.25 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240)	**36** (5180), **38** (5190), **40** (5200), **42** (5210), **44** (5220), **46** (5230), **48** (5240)	**36** (5180), **37** (5185), **38** (5190), **39** (5195), **40** (5200), **41** (5205), **42** (5210), **43** (5215), **44** (5220), **45** (5225), **46** (5230), **47** (5235), **48** (5240)
Japan2 (JP2)	5.25 - 5.35 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240)	**36** (5180), **38** (5190), **40** (5200), **42** (5210), **44** (5220), **46** (5230), **48** (5240)	**36** (5180), **37** (5185), **38** (5190), **39** (5195), **40** (5200), **41** (5205), **42** (5210), **43** (5215), **44** (5220), **45** (5225), **46** (5230), **47** (5235), **48** (5240)
Korea Republic (KR)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	10 MHz	5 MHz
Korea Republic2 (KR2)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)
Latvia (LV)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Liechtenstein (LI)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Lithuania (LT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	10 MHz	5 MHz
Luxembourg (LU)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Macau (MO)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Malaysia (MY)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Malta (MT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Mexico (MX)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	**10 MHz**	**5 MHz**
Netherlands (NL)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
New Zealand (NZ)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
North Korea (KP)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)
Norway (NO)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Panama (PA)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	**10 MHz**	**5 MHz**
Philippines (PH)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Poland (PL)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Portugal (PT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Puerto Rico (PR)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)

Country (Code)	**Frequency Bands**	**DFS**	**Allowed Channels (Center Freq)**		
			20 MHz	**10 MHz**	**5 MHz**
Russia (RU)	5.15 - 5.85 GHz	No	**30** (5150), **34** (5170), **38** (5190), **42** (5210), **46** (5230), **50** (5250), **54** (5270), **58** (5290), **62** (5310), **66** (5330), **70** (5350), **74** (5370), **78** (5390), **82** (5410), **86** (5430), **90** (5450), **94** (5470), **98** (5490), **102** (5510), **106** (5530), **110** (5550), **114** (5570), **118** (5590), **122** (5610), **126** (5630), **130** (5650), **134** (5670), **138** (5690), **142** (5710), **146** (5730), **150** (5750), **154** (5770), **158** (5790), **162** (5810), **166** (5830), **170** (5850)	**30** (5150), **32** (5160), **34** (5170), **36** (5180) **38** (5190), **40** (5200), **42** (5210), **44** (5220), **46** (5230), **48** (5240), **50** (5250), **52** (5260), **54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **68** (5340), **70** (5350), **72** (5360), **74** (5370), **76** (5380), **78** (5390), **80** (5400), **82** (5410), **84** (5420), **86** (5430), **88** (5440), **90** (5450), **92** (5460), **94** (5470), **96** (5480), **98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710), **144** (5720), **146** (5730), **148** (5740), **150** (5750), **152** (5760), **154** (5770), **156** (5780), **158** (5790), **160** (5800), **162** (5810), **164** (5820), **166** (5830), **168** (5840), **170** (5850)	**30** (5150), **31** (5155), **32** (5160), **33** (5165), **34** (5170), **35** (5175), **36** (5180), **37** (5185), **38** (5190), **39** (5195), **40** (5200), **41** (5205), **42** (5210), **43** (5215), **44** (5220), **45** (5225), **46** (5230), **47** (5235), **48** (5240), **49** (5245), **50** (5250), **51** (5255), **52** (5260), **53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **68** (5340), **69** (5345), **70** (5350), **71** (5355), **72** (5360), **73** (5365), **74** (5370), **75** (5375), **76** (5380), **77** (5385), **78** (5390), **79** (5395), **80** (5400), **81** (5405), **82** (5410), **83** (5415), **84** (5420), **85** (5425), **86** (5430), **87** (5435), **88** (5440), **89** (5445), **90** (5450), **91** (5455), **92** (5460), **93** (5465), **94** (5470), **95** (5475), **96** (5480), **97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710), **143** (5715), **144** (5720), **145** (5725), **146** (5730), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835), **168** (5840), **169** (5845), **170** (5850)
Saudi Arabia (SA)	5.15 - 5.35 GHz and 5.725 - 5.825 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240), **52** (5260), **56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)	**36** (5180), **38** (5190), **40** (5200), **42** (5210), **44** (5220), **46** (5230), **48** (5240), **50** (5250), **52** (5260), **54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**36** (5180), **37** (5185), **38** (5190), **39** (5195), **40** (5200), **41** (5205), **42** (5210), **43** (5215), **44** (5220), **45** (5225), **46** (5230), **47** (5235), **48** (5240), **49** (5245), **50** (5250), **51** (5255), **52** (5260), **53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	10 MHz	5 MHz
Singapore (SG)	5.15 - 5.25 GHz and 5.725 - 5.85 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**36** (5180), **38** (5190), **40** (5200), **42** (5210), **44** (5220), **46** (5230), **48** (5240), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**36** (5180), **37** (5185), **38** (5190), **39** (5195), **40** (5200), **41** (5205), **42** (5210), **43** (5215), **44** (5220), **45** (5225), **46** (5230), **47** (5235), **48** (5240), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Slovak Republic (SK)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Slovenia (SI)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
South Africa (ZA)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)

Country (Code)	**Frequency Bands**	**DFS**	**Allowed Channels (Center Freq)**		
			20 MHz	**10 MHz**	**5 MHz**
Spain (ES)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Sweden (SE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Switzerland (CH)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
Taiwan (158)	5.25 - 5.35 GHz and 5.725 - 5.825 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)
Thailand (TH)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)		
			20 MHz	**10 MHz**	**5 MHz**
United Kingdom (GB)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)	**98** (5490), **100** (5500), **102** (5510), **104** (5520), **106** (5530), **108** (5540), **110** (5550), **112** (5560), **114** (5570), **116** (5580), **118** (5590), **120** (5600), **122** (5610), **124** (5620), **126** (5630), **128** (5640), **130** (5650), **132** (5660), **134** (5670), **136** (5680), **138** (5690), **140** (5700), **142** (5710)	**97** (5485), **98** (5490), **99** (5495), **100** (5500), **101** (5505), **102** (5510), **103** (5515), **104** (5520), **105** (5525), **106** (5530), **107** (5535), **108** (5540), **109** (5545), **110** (5550), **111** (5555), **112** (5560), **113** (5565), **114** (5570), **115** (5575), **116** (5580), **117** (5585), **118** (5590), **119** (5595), **120** (5600), **121** (5605), **122** (5610), **123** (5615), **124** (5620), **125** (5625), **126** (5630), **127** (5635), **128** (5640), **129** (5645), **130** (5650), **131** (5655), **132** (5660), **133** (5665), **134** (5670), **135** (5675), **136** (5680), **137** (5685), **138** (5690), **139** (5695), **140** (5700), **141** (5705), **142** (5710)
United Kingdom 5.8 GHz (GB1)	5.725 - 5.85 GHz	Yes	**147** (5735), **151** (5755), **155** (5775), **167** (5835)	**145** (5725), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **163** (5815), **165** (5825), **167** (5835), **169** (5845)	**145** (5725), **146** (5730), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835), **168** (5840), **169** (5845), **170** (5850)
United States (US)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)	**54** (5270), **56** (5280), **58** (5290), **60** (5300), **62** (5310), **64** (5320), **66** (5330), **147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815), **165** (5825), **167** (5835)	**53** (5265), **54** (5270), **55** (5275), **56** (5280), **57** (5285), **58** (5290), **59** (5295), **60** (5300), **61** (5305), **62** (5310), **63** (5315), **64** (5320), **65** (5325), **66** (5330), **67** (5335), **147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815), **164** (5820), **165** (5825), **166** (5830), **167** (5835)
Uruguay (UY)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)
Venezuela (VE)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)	**147** (5735), **149** (5745), **151** (5755), **153** (5765), **155** (5775), **157** (5785), **159** (5795), **161** (5805), **163** (5815)	**147** (5735), **148** (5740), **149** (5745), **150** (5750), **151** (5755), **152** (5760), **153** (5765), **154** (5770), **155** (5775), **156** (5780), **157** (5785), **158** (5790), **159** (5795), **160** (5800), **161** (5805), **162** (5810), **163** (5815)

B Technical Specifications

Please see the following sections:

Part Numbers

North America Region

Model 2454-R

Base Station Unit

Part Number	Description
2454-BSUR-US-WORLD	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – US PSU -WORLD

Subscriber Unit

Part Number	Description
2454-SUA-US-WORLD	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – US PSU -WORLD
2454-SUR-US-WORLD	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – US PSU -WORLD

Model 5054-R

Base Station Unit

Part Number	Description
5054-BSUR-US	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – US PSU

Subscriber Unit

Part Number	Description
5054-SUA-US	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – US PSU
5054-SUR-US	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – US PSU

Europe and Middle East Regions

Model 2454-R

Base Station Unit

Part Number	Description
2454-BSUR-EU	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – Europe PSU
2454-BSUR-UK	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – UK PSU

Subscriber Unit

Part Number	Description
2454-SUA-EU	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – Europe PSU
2454-SUA-UK	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – UK PSU
2454-SUR-EU	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – Europe PSU
2454-SUR-UK	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – UK PSU

Model 5054-R

Base Station Unit

Part Number	Description
5054-BSUR-EU	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – Europe PSU
5054-BSUR-UK	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – UK PSU

Subscriber Unit

Part Number	Description
5054-SUA-EU	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – Europe PSU
5054-SUA-UK	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – UK PSU
5054-SUR-EU	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – Europe PSU
5054-SUR-UK	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – UK PSU

Asia Pacific Region

Model 2454-R

Base Station Unit

Part Number	Description
2454-BSUR-AU	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – Australia PSU
2454-BSUR-UK	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – UK PSU
2454-BSUR-US	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – US PSU
2454-BSUR-EU	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – Europe PSU
2454-BSUR-CN	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – China PSU
2454-BSUR-SK	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – South Korea PSU
2454-BSUR-US-WORLD	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – US/CAN PSU – WORLD

Subscriber Unit

Part Number	Description
2454-SUA-AU	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – Australia PSU
2454-SUA-UK	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – UK PSU
2454-SUA-US	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – US PSU
2454-SUA-EU	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – EU PSU
2454-SUA-CN	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – China PSU
2454-SUA-SK	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – South Korea PSU
2454-SUA-US WORLD	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – US/CAN PSU – WORLD

Part Number	Description
2454-SUR-AU	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – Australia PSU
2454-SUR-UK	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – UK PSU
2454-SUR-US	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – US PSU
2454-SUR-EU	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – EU PSU
2454-SUR-CN	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – China PSU
2454-SUR-SK	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – South Korea PS
2454-SUR-US-WORLD	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 16-dBi Antenna – US/CAN PSU - WORLD

Model 5054-R

Base Station Unit

Part Number	Description
5054-BSUR-AU	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – Australia PSU
5054-BSUR-UK	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – UK PSU
5054-BSUR-US	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – US PSU
5054-BSUR-EU	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – Europe PSU
5054-BSUR-US-WORLD	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – US/CAN PSU - WORLD

Subscriber Unit

Part Number	Description
5054-SUA-AU	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – Australia PSU
5054-SUA-UK	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – UK PSU
5054-SUA-US	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – US PSU
5054-SUA-EU	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – EU PSU
5054-SUA-US-WORLD	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – US/CAN PSU - WORLD
5054-SUR-AU	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – Australia PSU
5054-SUR-UK	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – UK PSU
5054-SUR-US	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – US PSU
5054-SUR-EU	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – EU PSU
5054-SUR-US-WORLD	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – US/CAN PSU - WORLD

Caribbean and Latin America Region

Model 2454-R

Base Station Unit

Part Number	Description
2454-BSUR-US	Tsunami MP.11 Model 2454-R Base Station Unit with Type-N Connector – US PSU

Subscriber Unit

Part Number	Description
2454-SUA-US	Tsunami MP.11 Model 2454-R Subscriber Unit with Type-N Connector – US PSU
2454-SUR-US	Tsunami MP.11 Model 2454-R Subscriber Unit with Integrated 23-dBi Antenna – US PSU

Model 5054-R

Base Station Unit

Part Number	Description
5054-BSUR-US	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – US PSU
5054-BSUR-BR	Tsunami MP.11 Model 5054-R Base Station Unit with Type-N Connector – Brazil PSU

Subscriber Unit

Part Number	Description
5054-SUA-US	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – US PSU
5054-SUA-BR	Tsunami MP.11 Model 5054-R Subscriber Unit with Type-N Connector – Brazil PSU
5054-SUR-US	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – US PSU
5054-SUR-BR	Tsunami MP.11 Model 5054-R Subscriber Unit with Integrated 23-dBi Antenna – Brazil PSU

Universal

Accessories

Part Number	Description
848 274 163	Surge Arrestor 0-3 GHz - Standard-N Female to Female
5054-SURGE	Surge Arrestor 5 GHz - Standard-N Female to Female
848 274 171	20 ft Low Loss Antenna Cable St-N - Male-Male LMR 200
848 332 789	20 ft Low Loss Antenna Cable St-N - Male-Male LMR 400
848 274 197	50 ft Low Loss Antenna Cable St-N - Male-Male LMR 400
848 274 205	75 ft Low Loss Antenna Cable St-N - Male-Male LMR 400
69828	6 ft Low Loss Antenna Cable St-N - Male-Male LMR 600
5054-LMR600-50	50 ft Low Loss Antenna Cable St-N - Male-Male LMR 600
70251	PoE (Power over Ethernet) Surge Arrestor for Tsunami MP.11 and QuickBridge.11

Outdoor Ethernet Cables

Part Number	Description
69819	25m outdoor, terminated CAT5 cable for Tsunami MP.11 or QB.11 with three RJ-45 and one weather-proof Ethernet port cap
69820	50m outdoor, terminated CAT5 cable for Tsunami MP.11 or QB.11 with three RJ-45 and one weather-proof Ethernet port cap
69821	75m outdoor, terminated CAT5 cable for Tsunami MP.11 or QB.11 with three RJ-45 and one weather-proof Ethernet port cap

Power Injector

Part Number	Description
69823	Spare Power DC Injector for Tsunami MP.11 or QB.11 (-R model ONLY)

2.4 GHz Antennas

Part Number	Description
848 515 722	5 dBi Omni-Directional Vehicle Antenna w/Integrated 250 cm cable
848 312 591	7 dBi Omni-Directional Base Station Antenna - St-N Female
848 515 698	10 dBi Omni-Directional Base Station Antenna - St-N Female
848 515 706	12 dBi Directional Wide Angle Antenna (120 degrees) - St-N Female
2411WA12-STN	12 dBi Wide Angle Antenna with Integrated 2 m cable (st-N) Mountable on Window or Flat Surface
848 515 714	24 dBi Directional Antenna (Parabolic Grid) - St-N Female
2400-SA60-14	14dBi Directional sector antenna (60 degrees) 2.4GHz St-N Female

5 GHz Antennas

Part Number	Description
5054-PA-18	18 dBi Panel Antenna - St-N Female - 5.25 - 5.875 GHz
5054-PA-23	23 dBi Panel Antenna - St-N Female - 5.725 - 5.875 GHz
5054-OA-8	8 dBi Omni Directional Antenna - St-N Female - 5.47-5.850 GHz
5054-OA-10	10 dBi Omni Directional Antenna - St-N Female - 5.47-5.850 GHz
5054-SA120-14	14 dBi Sector Antenna - St-N Female - 5.25-5.850 GHz - 120 degrees
5054-SA60-17	17 dBi Sector Antenna - St-N Female - 5.25-5.850 GHz - 60 degrees

Regulatory Approvals and Frequency Ranges

Model 2454-R Regulatory Approval and Frequency Ranges

Region/Country	Country	GHz	Number of Channels			Certification
			5 MHz	10 MHz	20 MHz	
North America	USA	2.40 - 2.4835	11	Up to 11	Up to 11	Yes
		2.40 - 2.472	13	Up to 13	Up to 13	Yes
	Canada	2.40 - 2.4835	11	Up to 11	Up to 11	Yes
		2.40 - 2.472	13	Up to 13	Up to 13	Yes
	Mexico	2.40 - 2.4835	11	Up to 11	Up to 11	Yes
		2.40 - 2.472	13	Up to 13	Up to 13	Yes
EU Countries	Austria	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Belgium	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Cyprus	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Czech Republic	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Denmark	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Estonia	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Finland	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	France	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Germany	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Greece	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Hungary	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Ireland	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Italy	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Latvia	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Luxemburg	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Lithuania	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Malta	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Netherlands	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Poland	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Portugal	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Spain	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Sweden	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Slovakia	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Slovenia	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	United Kingdom	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
Other European Countries	Iceland	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Liechtenstein	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Norway	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Switzerland	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
South America	Brazil	2.40 - 2.4835	13	Up to 13	Up to 13	In Process

Model 2454-R Regulatory Approval and Frequency Ranges (continued)

Region/Country	Country	GHz	Number of Channels			Certification
			5 MHz	10 MHz	20 MHz	
APAC	New Zealand	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Japan	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Hong Kong	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	S. Korea	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	China	2.40 - 2.4835	13	Up to 13	Up to 13	Yes
	Taiwan	2.40 - 2.4835	13	Up to 13	Up to 13	Yes

Model 5054-R Regulatory Approval and Frequency Ranges

Region/Country	Country	GHz	Number of Channels			Certification
			5 MHz	10 MHz	20 MHz	
North America	USA	5.25 - 5.35	Up to 15	Up to 7	Up to 3	Yes
		5.725 - 5.85	Up to 21	Up to 11	Up to 5	
	Canada	5.25 - 5.35	Up to 15	Up to 7	Up to 3	Yes
		5.725 - 5.85	Up to 21	Up to 11	Up to 5	
	Mexico	5.725 - 5.85	Up to 21	Up to 11	Up to 5	Yes
EU Countries	Austria	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Belgium	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Cyprus	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Czech Republic	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Denmark	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Estonia	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Finland	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	France	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Germany	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Greece	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Hungary	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Ireland	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
		5.725 - 5.85	Up to 23	Up to 11	Up to 4	
	Italy	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Latvia	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Lithuania	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Luxemburg	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Malta	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Netherlands	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Poland	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Portugal	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Slovakia	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Slovenia	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Spain	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Sweden	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	United Kingdom	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
		5.725 - 5.85	Up to 23	Up to 11	Up to 4	
Other European Countries	Iceland	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Liechtenstein	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Norway	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
	Russia	5.15 - 5.85	Up to 141	Up to 71	Up to 36	In Process
	Switzerland	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes

Model 5054-R Regulatory Approval and Frequency Ranges (continued)

Region/Country	Country	GHz	Number of Channels			Certification
			5 MHz	10 MHz	20 MHz	
South America	Argentina	5.25 - 5.35	Up to 9	Up to 5	Up to 3	Yes
		5.725 - 5.85	Up to 19	Up to 10	Up to 5	
	Brazil	5.47 - 5.70	Up to 46	Up to 23	Up to 11	Yes
		5.725 - 5.85	Up to 19	Up to 10	Up to 5	
	Colombia	5.25 - 5.35	Up to 15	Up to 7	Up to 3	Yes
		5.725 - 5.85	Up to 21	Up to 11	Up to 5	
APAC	Australia	5.725 - 5.85	Up to 21	Up to 11	Up to 5	Yes
	China	5.725 - 5.85	Up to 17	Up to 9	Up to 5	Yes
	Hong Kong	5.725 - 5.85	Up to 21	Up to 11	Up to 5	Yes
	India	5.15 - 5.35	Up to 32	Up to 16	Up to 7	In Process
		5.725 - 5.85	Up to 17	Up to 9	Up to 5	
	New Zealand	5.725 - 5.85	Up to 21	Up to 11	Up to 5	Yes
	S. Korea	5.725 - 5.85	Up to 17	Up to 9	Up to 5	Yes
	Singapore	5.15 - 5.25	Up to 13	Up to 7	Up to 4	In Process
		5.725 - 5.85	Up to 17	Up to 9	Up to 5	
	Taiwan	5.25 - 5.35	Up to 15	Up to 7	Up to 3	Yes
		5.725 - 5.85	Up to 17	Up to 9	Up to 5	

Integrated Antenna Specification

Model 2454-R

Subscriber Unit with Integrated 16-dBi Antenna

Feature	Specification
Part Number	2454-SUR-xx
Frequency range	2.4 to 2.5 GHz
Nominal Impedance	50 Ohms
Gain	16 dBi
Front-to-Back Ratio	25 dB
HPBW/vertical	22 degrees
HPBW/horizontal	15 degrees
Cross Polarization	20 dB
Power handling	1 W
VSWR	1.5 : 1 Max

Model 5054-R

Subscriber Unit with Integrated 23-dBi Antenna

Feature	Specification
Part Number	5054-SUR-xx
Frequency range	5250 - 5875 MHz
Nominal Impedance	50 ohms
Gain	23 dBi
Front-to-Back Ratio	35 dB
HPBW/vertical	9 degrees
HPBW/horizontal	9 degrees
Cross Polarization	23 dB
Power handling	1 W (cw)
VSWR	2.0 : 1 Max

RF Modulation and Over-the-Air Rates

Model 2454-R and 5054-R OFDM (Orthogonal Frequency Division Multiplexing)

- Maximum Packet Size 1522 Bytes
- Modulation Rates:

Modulation	Rate		
	20 MHz Channels	10 MHz Channels	5 MHz Channels
BPSK	6 and 9 Mbps	3 and 4.5 Mbps	2.25 and 1.5 Mbps
QPSK	12 and 18 Mbps	6 and 9 Mbps	3 and 4.5 Mbps
16-QAM	24 and 36 Mbps	12 and 18 Mbps	6 and 9 Mbps

Wireless Protocol

- Worp (Wireless Outdoor Router Protocol)

Device Interface

- Ethernet: Auto-sensing 10/100BASE-TX Ethernet
- Antenna Connector for BSU and SU with Type-N Connector: Standard Type-N Female

Network Architecture Type

- Infrastructure

Receive Sensitivity

- BER=10-6

2454-R/5054-R

Modulation	40 MHz Channels Turbo Mode (US only)	20 MHz Channels Standard Mode	10 MHz Channels Standard Mode	5 MHz Channels Standard Mode
64QAM ¾	-66 dBm @108Mbps	-69 dBm @54Mbps	-72 dBm @36Mbps	-75 dBm @18Mbps
64QAM ½	-68 dBm @96Mbps	-72 dBm @48Mbps	-75 dBm @24Mbps	-78 dBm @12Mbps
16QAM ¾	-75dBm @72Mbps	-77 dBm @36Mbps	-80 dBm @18Mbps	-83 dBm @9Mbps
16QAM ½	-78dBm @48Mbps	-80 dBm @24Mbps	-83 dBm @12Mbps	-86 dBm @6Mbps
QPSK ¾	-81dBm @36Mbps	-83 dBm @18Mbps	-86 dBm @9Mbps	-89 dBm @4.5Mbps
QPSK ½	-83 dBm @24Mbps	-86 dBm @12Mbps	-89 dBm @6Mbps	92 dBm @3Mbps
BPSK ¾	-84 dBm @18Mbps	-87 dBm @9Mbps	-90 dBm @4.5Mbps	-93 dBm @2.25Mbps
BPSK ½	-85 dBm @12Mbps	-88 dBm @6Mbps	-91 dBm @3Mbps	-94 dBm @1.5Mbps

Maximum Throughput

2454-R

Data Rate	20 MHz Channels	10 MHz Channels	5 MHz Channels Standard Mode
54 Mbps	30 Mbps	—	—
48 Mbps	28 Mbps	—	—
36 Mbps	18 Mbps	—	—
24 Mbps	14 Mbps	—	—
18 Mbps	12 Mbps	12 Mbps	—
12 Mbps	9 Mbps	9 Mbps	—
9 Mbps	7 Mbps	7 Mbps	6.8 Mbps
6 Mbps	5 Mbps	5 Mbps	5 Mbps
4.5 Mbps	—	4 Mbps	4 Mbps
3 Mbps	—	2 Mbps	2.7 Mbps
2.25 Mbps	—	—	2 Mbps
1 Mbps	—	—	1.4 Mbps

Note: Maximum-throughput data with release 2.3, as measured with test equipment under controlled lab conditions and best performing packet size. In some instances, data compression yields throughput equal to the configured data rate. Actual throughput performance in the field may vary.

5054-R

Data Rate	40 MHz Channels (US Only)	20 MHz Channels	10 MHz Channels	5 MHz Channels Standard Mode
108 Mbps Turbo 54	31 Mbps	—	—	—
96 Mbps Turbo 48	28 Mbps	—	—	—
72 Mbps Turbo 36	28 Mbps	—	—	—
48 Mbps Turbo 24	28 Mbps	—	—	—
36 Mbps Turbo 18	24 Mbps	—	—	—
24 Mbps Turbo 12	19 Mbps	—	—	—
54 Mbps	—	29 Mbps	—	—
48 Mbps	—	27 Mbps	—	—
36 Mbps	—	22 Mbps	—	—
24 Mbps	—	16 Mbps	16 Mbps	—
18 Mbps	—	13 Mbps	13 Mbps	—
12 Mbps	—	9 Mbps	9 Mbps	—
9 Mbps	—	7 Mbps	7 Mbps	7 Mbps
6 Mbps	—	5 Mbps	5 Mbps	4.7 Mbps
4.5 Mbps	—	—	3.6 Mbps	3.8 Mbps
3 Mbps	—	—	2.4 Mbps	2.7 Mbps

Data Rate	40 MHz Channels (US Only)	20 MHz Channels	10 MHz Channels	5 MHz Channels Standard Mode
2.25 Mbps	—	—	—	2 Mbps
1 Mbps	—	—	—	1.2 Mbps

Note: Maximum-throughput data with release 2.3, as measured with test equipment under controlled lab conditions and best performing packet size. In some instances, data compression yields throughput equal to the configured data rate. Actual throughput performance in the field may vary.

Latency

- < 10ms typical at maximum throughput (as measured with test equipment under controlled lab conditions and best performing packet size)

Transmit Power Settings

Model 2454-R

- Output Power Attenuation: 0 - 18dB, in 3dB steps
- Output Power Values will have a tolerance of +- 1.5 dB

Frequency	**6-24 Mbps @ 20 MHz** 16QAM ½; QPSK ¾; QPSK ½; BPSK ¾; BPSK ½	**36 Mbps @ 20 MHz** 16QAM ¾	**48 Mbps @ 20 MHz** 64QAM ½	**54 Mbps @ 20 MHz** 64QAM ¾
2.400-2.483 GHz	16 dBm	16 dBm	14 dBm	13 dBm

Model 5054-R

- Output Power Attenuation: 0 - 18dB, in 3dB steps
- Output Power Values will have a tolerance of +- 1.5 dB

Frequency	**6-24 Mbps @ 20 MHz** 16QAM ½; QPSK ¾; QPSK ½; BPSK ¾; BPSK ½	**36 Mbps @ 20 MHz** 16QAM ¾	**48 Mbps @ 20 MHz** 64QAM ½	**54 Mbps @ 20 MHz** 64QAM ¾
5.15-5.35 GHz	15 dBm	13 dBm	12 dBm	11 dBm
5.47-5.725 GHz	16 dBm	13 dBm	12 dBm	11 dBm
5.725-5.850 GHz	16 dBm	13 dBm	12 dBm	11 dBm

Range Information

Model 2454-R

Integrated Antenna

Frequency	36 Mbps	6 Mbps
2.4-2.4835GHz (US)	2.1mi/3.4km	6.9mi/11.1km
2.4-2.8 GHz (ETSI)	0.7mi/1.1km	2.6mi/4.2km

External Antenna

Frequency	36 Mbps	6 Mbps
2.4-2.4835GHz (US)	3.4mi/5.5km	11.4mi/18.3km
2.4-2.8 GHz (ETSI)	0.7mi/1.1km	2.6mi/4.2km

Model 5054-R

Integrated Antenna

Frequency	36 Mbps	6 Mbps
5.15-5.35 GHz (US)	1.2mi/2.0km	3.0mi/4.8km
5.47-5.7GHz (ETSI)	1.1mi/1.8km	3.1mi/5.0km
5.725-5.850 (US)	2.1mi/3.8km	6.4mi/10.3km

External Antenna

Frequency	36 Mbps	6 Mbps
5.15-5.35 GHz (US)	1.2mi/2.0km	3.2mi/5.1km
5.47-5.7GHz (ETSI)	1.1mi/1.8km	3.1mi/5.0km
5.725-5.850 (US)	4.1mi/6.6km	12.5mi/20.1km

Notes

Note the following:

- PMP configuration using USA regulations for L and U bands, ETSI regulations for M bands
- Clear LOS
- 99.995% availability
- Sector antenna (17dBi, 60-degrees) at BSU with short 1dB jumper cable
- Fade margin minimum of 10dB to 2 miles, 0.2dB additional fade margin for every 0.1 mile to 15dB
- Predicted availability >99.990% (one-way) for all configurations
- Distance calculations for 5 and 10 MHz channels are comparable for ETSI regulatory domains. Proper TPC settings (3 and 6dB) respectively, should be set to meet power density rules. Increased distances are possible in the US with proper link engineering.

System Processor and Memory

- 166MHz Motorola 8241 processor
- 16 Mbytes RAM

- 8 Mbytes FLASH

Software Specification

Base Station and Subscriber Units

- Miscellaneous
  - WORP protocol
  - Dynamic Data Rate Selection
  - Transmit Power Control
  - Antenna Alignment
  - Integrity Check for Software Upload
  - 5, 10, and 20MHz channels
- Satellite Density
  - Dynamic Frequency Selection
- Redundancy
  - Spanning Tree (802.1D)
- Bridging and Routing
  - Bridge (802.1d)
  - IP/ RIPv1 (RFC 1058)
  - IP/ RIPv2 (RFC 1388)
  - CIDR (RFC 1519)
  - ICMP (RFC 792)
  - IP (RFC 791)
  - ARP (RFC 826)
- Filtering
  - Ethernet protocol (Ethertype)
  - Static MAC
  - Storm threshold
  - IP address
  - Broadcast protocol
- Services
  - DHCP Server (RFC 2131)
  - DHCP Client (RFC 2131)
  - Bi-Directional Bandwidth Control
- VLAN
  - 802.1Q
- Security Features
  - MAC Authentication
  - Radius MAC Access Control
  - WEP/AES-OCB encryption
  - RADIUS (RFC 2138)
- Mobility
  - Subscriber Unit Roaming

Base Station Unit

- Filtering
  - Intra Cell Blocking

Subscriber Units

- Services
  - NAT (RFC 3022)
  - DHCP Relay (RFC 2131)

Security

- WORP provides critical feature support for secure long-range wireless deployments in unlicensed frequency spectrum.
- MD5 (embedded in WORP) authentication between BSU and SU.
- Filter based on packet information such as unicast/multicast/ broadcast MAC or IP.
- Secure “over the air encryption” with WEP, WEP+, and AES, and AES-CCB.
- Authentication via Radius
- Intracell blocking allows the BSU to act as the central policy enforcer for SU to SU communications.

Management

- SU/BSU statistics
- Link Test
- Temperature logging
- SNMPv1/v2 RFC 1157
- SNMP v2c (RFC 1907)
- HTTP Server (RFC 2616)
- Telnet (RFC 855)
- TFTP client (RFC 783)
- CLI
- MIB-II (RFC 1213)
- Ethernet-like MIB (RFC 1643)
- Bridge MIB (RFC 1493)
- 802.3MAU (RFC 2668)
- 802.11 MIB
- Remote reboot (reload) or reset to factory default via power injector
- Private MIB
- Orinoco MIB

Antenna

- Audible tone
- CLI output

Status LEDs

- Two indicators on the RJ-45 connector to indicate power, wireless traffic, and Ethernet traffic

Local Configuration Support

- RS-232 Serial port
  – RJ11 port built-into the unit
  – DB9 Female via a converter (included)

Compliance and Standards

Safety

- UL: 60950, UL50
- CSA: 22.2 No. 60950-00
- IEC: 60950 3rd Ed (1999)

Radio Approvals

- USA: FCC 15.107, 15-109; 15-203-15.205, 15.207, 15.209; 15.247; 15.401-15.407
- Canada: RSS-102; RSS-210; ICES-003
- Europe (ETSI): EN 301.893; EN 300.328; EN 301.489-1; EN 301.489-17; EN 300-440; EN50371
- ARIB: STD-T71, STD 33, STD 66

EMI and Susceptibility (Class B)

- USA: FCC Part 15.107
- Canada: ICES-003

Water and Dust Proof

- NEMA4/IP56

Electrical

5054-R / 2454-R POE Power Injector

- Custom Power over Ethernet (802.3af compatible)
- Input: Voltage 110 to 250 VAC (47-63Hz)
- Output: 48V @ 420mA MAX (injected into the Cat-5 Cable)
- Pin for Remote reboot (reload) or reset to factory default

5054-R / 2454-R Outdoor Radio Unit

- Power Consumption: 7.5W typical. Up to 20 Watts across full operating temperature range.
- Input: Voltage 42 to 60 VDC

Dimensions

Base Station and Subscriber Unit

- Packaged: 14.57 in x 13.70 in x 8.19 in (370 mm x 348 mm x 208 mm)

Base Station and Subscriber Unit with Type-N Connector

- Unpackaged: 10.5 in x 10.5 in x 3.25 in (267 mm x 267 mm x 83 mm)

Subscriber Unit with Integrated 23-dBi Antenna

- Unpackaged: 12.60 in x 12.60 in x 3.50 in (320 mm x 320 mm x 89 mm)

Weight

Base Station and Subscriber Unit with Type-N Connector

- Packaged weight: 9.2 lbs (4.2 kg)
- Unpackaged weight: 5.5 lbs (2.49 kg) Unit-only, .45 lbs (.20 kg) for power supply

Subscriber Unit with Integrated 23-dBi or 16-dBi Antenna

- Packaged weight: 10.1 lbs (4.6 kg)
- Unpackaged weight: 6.0 lbs (2.72 kg) Unit-only, .45 lbs (.20 kg) for power supply

Environmental

Operating

- -33º to 60ºC (-27.5º to 140º Fahrenheit)
- 100% humidity
- Wind loading: 125 mph

Storage

- -55º to 80ºC (-41º to 176º Fahrenheit)
- 100% humidity

Packaging Contents

- One Tsunami MP.11 Model 2454-R or 5054-R Base Station or Subscriber Unit
- One wall/ pole mounting bracket
- One Power-Over-Ethernet injector for Model 2454-R or 5054-R
- One country specific power cord
- One Ethernet cable weather-proof plug
- One Documentation and Software CD-ROM

MTBF

- 100,000 hours

Warranty

- One year

C
Lightning Protection

Lightning protection is used to maximize the reliability of communications equipment by safely re-directing current from a lightning strike or a power surge traveling along the Cat 5 Ethernet cabling to ground using the shortest path possible. Designing a proper grounding system prior to installing any communications equipment is critical to minimize the possibility of equipment damage, void warranties, and cause serious injury.

The surge arrestor (sometimes referred to as a lightning protector) can protect your sensitive electronic equipment from high-voltage surges caused by discharges and transients at the PoE.

Proxim Wireless offers superior lightning and surge protection for Tsunami MP.11 and Tsunami QuickBridge.11 products. Contact your reseller or distributor for more information.

Technical Services and Support

D

Obtaining Technical Services and Support

If you are having trouble utilizing your Proxim product, please review this manual and the additional documentation provided with your product.

If you require additional support and would like to use Proxim's free Technical Service to help resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services:

- **Product information:**
  - Part number of suspected faulty unit
  - Serial number of suspected faulty unit
- **Trouble/error information**:
  - Trouble/symptom being experienced
  - Activities completed to confirm fault
  - Network information (what kind of network are you using?)
  - Circumstances that preceded or led up to the error
  - Message or alarms viewed
  - Steps taken to reproduce the problem
- **Servpak information (if a Servpak customer)**:
  - Servpak account number
- **Registration information**:
  - If the product is not registered, date when you purchased the product
  - If the product is not registered, location where you purchased the product

NOTE: *If you would like to register your product now, visit the Proxim eService Web Site at* http://support.proxim.com *and click on* **New Product Registration**.

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at http://support.proxim.com.

On the Proxim eService Web Site, you can access the following services:

- **New Product Registration**: Register your product for free support.
- **Open a Ticket or RMA**: Open a ticket or RMA and receive an immediate reply.
- **Search Knowledgebase**: Locate white papers, software upgrades, and technical information.
- **ServPak (Service Packages)**: Receive Advanced Replacement, Extended Warranty, 7x24x365 Technical Support, Priority Queuing, and On-Site Support.
- **Your Stuff**: Track status of your tickets or RMAs and receive product update notifications.
- **Provide Feedback**: Submit suggestions or other types of feedback.
- **Customer Survey**: Submit an On-Line Customer Survey response.
- **Repair Tune-Up**: Have your existing Proxim equipment inspected, tested, and upgraded to current S/W and H/W revisions, and extend your warranty for another year.

Telephone Support

Contact technical support via telephone as follows:

- **Domestic**: 866-674-6626
- **International**: +1-408-542-5390

Hours of Operation

- **North America**: 8 a.m. to 5 p.m. PST, Monday through Friday
- **EMEA**: 8 a.m. to 5 p.m. GMT, Monday through Friday

ServPak Support

Proxim understands that service and support requirements vary from customer to customer. It is our mission to offer service and support options that go above-and-beyond normal warranties to allow you the flexibility to provide the quality of service that your networks demand.

In recognition of these varying requirements we have developed a support program called ServPak. ServPak is a program of Enhanced Service Options that can be purchased individually or in combinations to meet your needs.

- **Advanced Replacement**: This service offers customers an advance replacement of refurbished or new hardware. (Available in the U.S., Canada, and select countries. Please inquire with your authorized Proxim distributor for availability in your country.)
- **Extended Warranty**: This service provides unlimited repair of your Proxim hardware for the life of the service contract.
- **7x24x365 Technical Support**: This service provides unlimited, direct access to Proxim's world-class technical support 24 hours a day, 7 days a week, 365 days a year.
- **Priority Queuing**: This service allows your product issue to be routed to the next available Customer Service Engineer.

To purchase ServPak support services, please contact your authorized Proxim distributor.   To receive more information or for questions on any of the available ServPak support options, please call Proxim Support at +1-408-542-5390 or send an email to servpak@proxim.com.

Statement of Warranty

E

Warranty Coverage

Proxim Wireless Corporation warrants that its Products are manufactured solely from new parts, conform substantially to specifications, and will be free of defects in material and workmanship for a Warranty Period of **1 year** from the date of purchase.

Repair or Replacement

In the event a Product fails to perform in accordance with its specification during the Warranty Period, Proxim offers return-to-factory repair or replacement, with a thirty (30) business-day turnaround from the date of receipt of the defective Product at a Proxim Wireless Corporation Repair Center. When Proxim Wireless has reasonably determined that a returned Product is defective and is still under Warranty, Proxim Wireless shall, at its option, either: (a) repair the defective Product; (b) replace the defective Product with a refurbished Product that is equivalent to the original; or (c) where repair or replacement cannot be accomplished, refund the price paid for the defective Product. The Warranty Period for repaired or replacement Products shall be ninety (90) days or the remainder of the original Warranty Period, whichever is longer. This constitutes Buyer's sole and exclusive remedy and Proxim Wireless's sole and exclusive liability under this Warranty.

Limitations of Warranty

The express warranties set forth in this Agreement will not apply to defects in a Product caused; (i) through no fault of Proxim Wireless during shipment to or from Buyer, (ii) by the use of software other than that provided with or installed in the Product, (iii) by the use or operation of the Product in an application or environment other than that intended or recommended by Proxim Wireless, (iv) by modifications, alterations, or repairs made to the Product by any party other than Proxim Wireless or Proxim Wireless's authorized repair partners, (v) by the Product being subjected to unusual physical or electrical stress, or (vii) by failure of Buyer to comply with any of the return procedures specified in this Statement of Warranty.

Support Procedures

Buyer should return defective LAN[1] Products within the first 30 days to the merchant from which the Products were purchased. Buyer can contact a Proxim Wireless Customer Service Center either by telephone or via web. Calls for support for Products that are near the end of their warranty period should be made not longer than seven (7) days after expiration of warranty. Repair of Products that are out of warranty will be subject to a repair fee. Contact information is shown below. Additional support information can be found at Proxim Wireless's web site at http://support.proxim.com.

- **Domestic**: 866-674-6626
- **International**: +1-408-542-5390

Hours of Operation

- **North America:** 8 a.m. to 5 p.m. PST, Monday through Friday
- **EMEA:** 8 a.m. to 5 p.m. GMT, Monday through Friday

When contacting the Customer Service for support, Buyer should be prepared to provide the Product description and serial number and a description of the problem. The serial number should be on the product.

In the event the Customer Service Center determines that the problem can be corrected with a software update, Buyer might be instructed to download the update from Proxim Wireless's web site or, if that's not possible, the update will be sent to Buyer. In the event the Customer Service Center instructs Buyer to return the Product to Proxim Wireless for

[1] LAN products include: ORiNOCO™

repair or replacement, the Customer Service Center will provide Buyer a Return Material Authorization ("RMA") number and shipping instructions. Buyer must return the defective Product to Proxim Wireless, properly packaged to prevent damage, shipping prepaid, with the RMA number prominently displayed on the outside of the container.

Calls to the Customer Service Center for reasons other than Product failure will not be accepted unless Buyer has purchased a Proxim Wireless Service Contract or the call is made within the first thirty (30) days of the Product's invoice date. Calls that are outside of the 30-day free support time will be charged a fee of $25.00 (US Dollars) per Support Call.

If Proxim Wireless reasonably determines that a returned Product is not defective or is not covered by the terms of this Warranty, Buyer shall be charged a service charge and return shipping charges.

Other Information

Search Knowledgebase

Proxim Wireless stores all resolved problems in a solution database at the following URL: http://support.proxim.com.

Ask a Question or Open an Issue

Submit a question or open an issue to Proxim Wireless technical support staff at the following URL: http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/ask.php.

Other Adapter Cards

Proxim Wireless does not support internal mini-PCI devices that are built into laptop computers, even if identified as "ORiNOCO" devices. Customers having such devices should contact the laptop vendor's technical support for assistance.

For support for a PCMCIA card carrying a brand name other than Proxim, ORiNOCO, Lucent, Wavelan, or Skyline, Customer should contact the brand vendor's technical support for assistance.